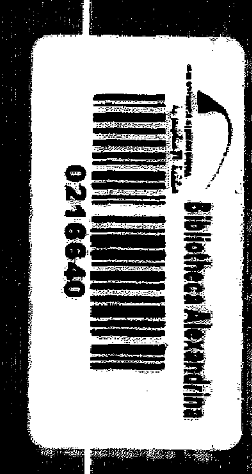


أكاديمية نايف العربية للعلوم الأمنية

مركز الدراسات والبحوث

جرائم نظم المعلومات

المهندس حسن طاهر داود



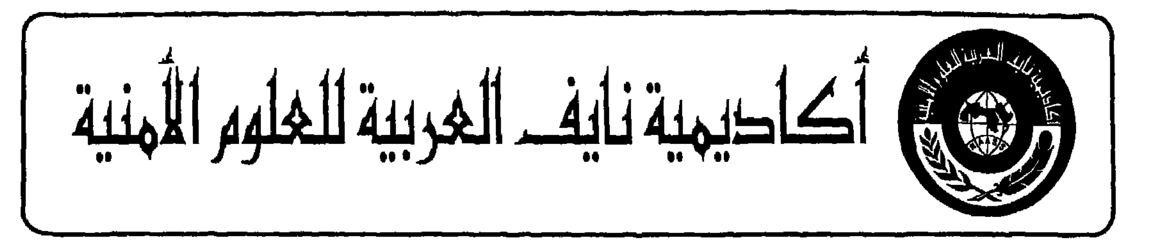


الريـــاض
١٤٢٠هـ ـ ٢٠٠٠م

اهداءات ٢٠٠٢

ا.د/ عبد العزيز بن صقر الغامدي

الرياض



جرائم نظم المعلومات

المهندس حسن طاهر داود

الطبعة الأولى

الريـــاض

١٤٢٠هـــ ٢٠٠٠م

المملكة العربية السعودية. ص.ب ٦٨٣٠ الرياض: ١١٤٥٢
هاتف ٢٤٦٣٤٤٤ (٩٦٦-١-) فاكس ٢٤٦٤٧١٣ (٩٦٦-١-)
البريد الإلكتروني: naassrc@ yahoo. Com.

ISBN 3-06-853-9960
P.O.Box: 6830 Riyadh 11452 Tel. (966+1) 2463444 KSA
Fax (966 + 1) 2464713 E-mail naassrc@ yahoo. Com.

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

داود، حسن طاهر

جرائم نظم المعلومات، - الرياض

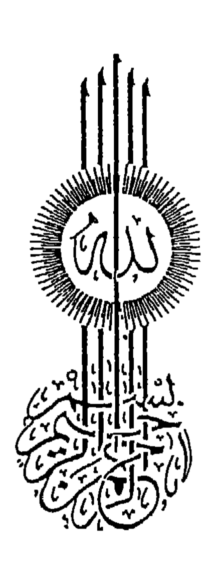
٢٤٤ص، ١٧ × ٢٤ سم

ردمك: ٣-٠٦-٨٥٣-٩٩٦٠

١ - نظم المعلومات　　　أ- العنوان

ديوي ٠٢٩,٧　　　٢٠/٢٢٨٨

رقم الايداع: ٢٠/٢٢٨٨
ردمك: ٣-٠٦-٨٥٣-٩٩٦٠



المحتويـــات

تقديـــــم

تهدف الأجهزة الأمنية وأجهزة العدالة الجنائية في مختلف الدول إلى منع الجريمة والعمل على الوقاية منهما بشتى السبل والوسائل. ولقد عرفت المجتمعات الإنسانية ومنها المنطقة العربية جرائم مختلفة واجهتها بأساليب متعددة ومتنوعة. لكن التطور التقني الذي تعيشه اليوم كافة مناطق العالم وبلدانه، والمتمثل باستخدام الكمبيوتر ونظم المعلومات، أدى إلى استحداث جرائم لم تكن معروفة من قبل، ولذا فهي كثيراً ما تدعى بالجرائم المستحدثة، وهي دون شك جرائم من نوع فريد، تحتاج إلى تشريعات خاصة، وإلى وسائل إثبات مختلفة عما ألفناه في الماضي، بل وإلى كفاءات مدربة ومؤهلة على نحو يجعلها قادرة على مواجهة ومكافحة هذا النوع من الجرائم.

انتشرت جرائم نظم المعلومات خلال السنوات الأخيرة في الدول الصناعية، ولم تعد منطقتنا العربية بمنأى عنها نتيجة التطور الكبير الذي تشهده الدول العربية، وازدياد استخدامها لنظم المعلومات في شتى الميادين العلمية والاقتصادية، إلى جانب استخدام الأنترنت على نحو متسارع. إننا نعيش عصر المعلومات الذي يقتضي من كافة الهيئات العلمية والأمنية العربية أن تبذل جهوداً علمية وعملية كبيرة للوقاية من جرائم نظم المعلومات، كما يستدعي من الجهات العربية المختصة أن تكون على مستوى الأحداث في إعداد البرامج، ووضع الخطط، واستحداث الأنظمة والتشريعات التي تساعد على مواجهة جرائم نظم المعلومات وردع مقترفيها.

إن أكاديمية نايف العربية للعلوم الأمنية إذ تقدم هذه الدراسة الهامة إلى الجهات العلمية والأمنية، وإلى الهيئات المعنية بالعدالة الجنائية في الدول العربية كافة، لتأمل أن يكون فيها ما يفيد لدعم جهود الوقاية من جرائم نظم المعلومات، كما تأمل أن تكون هذه الدراسة لبنة هامة ضمن الجهود العلمية المتميزة في هذا الميدان الذي يحتاج المزيد من الدراسات والبحوث.

والله من وراء القصد.

رئيس

أكاديمية نايف العربية للعلوم الأمنية

أ.د. عبدالعزيز بن صقر الغامـــدي

مقدمـــــة

الحمد لله . . والصلاة والسلام على رسول الله .

أهمية المعلومات ليست خافية على أحد، وككل ثمين فهي دائمًا في خطر . ولذلك لم يكن غريبًا أن يصبح أمن المعلومات هاجس الجميع، من منظمات وشركات وأفراد . لا سيما أن الجريمة تطورت تطوراً ادى إلى انتهاك حرمة المعلومات وتعريض أمنها الخطر الشديد، إلا أنه دفع الكثير إلى القلق على المعلومات والحرص على حمايتها وتأمينها وإبعادها عن أيدي العابثين .

وعلى المستوى الشخصي فإن رحلتي مع الحاسب الآلي ومع «أمن المعلومات» قد بدأت منذ أكثر من ثلاثين عاماً بين الممارسة والتدريب، مما جعلني أسعد بالدعوة الكريمة من الدكتور ذياب البداينة عميد مركز الدراسات والبحوث بأكاديمية نايف العربية للعلوم الأمنية لكي أنجز هذا الكتاب . لذا أود أن اشكره على نشاطه الملحوظ وعلى اهتمامه وتشجيعه للبحث العلمي .

هذا الكتاب يتناول موضوع «جرائم نظم المعلومات» وهي الجرائم التي يكون الحاسب موضوعها أو يكون وسيلتها . ولقد قسمت هذا الكتاب إلى أربعة عشر فصلاً، خصصت الفصلين الأولين منها لتوضيح خصائص عصر المعلومات والتعريف بهذا النوع من الجرائم، وأفردت الفصل الثالث لمجموعة كبيرة من أنواع جرائم نظم المعلومات بينما رأيت أن أفرد الفصل الخامس لجرائم التجسس المعلوماتي . ونظرًا لخطورة وأهمية شبكة الإنترنت والنوعية الجديدة من جرائم نظم المعلومات المتعلقة بها فقد كان لها نصيب كبير من هذا البحث، فخصصت الفصلين الخامس والسادس للأخطار التي تواجه الشبكة والجرائم التي ترتكب من خلالها . أما الفصل السابع فكان من نصيب «أمن البريد الإلكتروني»، وخصصت الفصل الثامن للحديث

عن مخاطر «تداول النقود الإلكترونية»، وكما ترون فهما أيضًا ليسا بعيدين عن شبكة الإنترنت. ولم يكن ممكنًا أن نتحدث عن جرائم نظم المعلومات دون أن نتعرض لأخطر ما شهدته البشرية من جرائم تصيب ضحاياها عشوائيًا دون أن يجني مرتكبها أي فائدة من ورائها في معظم الأحوال، وأعني بها «الفيروسات» فكان لها الفصل التاسع. ولما كنت شاهدًا في أحوال كثيرة على ما يسببه المبرمجون من أخطاء، ومن انتهاك لأمن المعلومات عند إعدادهم لبرامجهم، بحسن نية أحيانًا وبسوء نية في بعض الأحوال، لذلك حرصت على تخصيص فصل لهذا الموضوع كان هو الفصل العاشر. أما الفصل الحادي عشر فقد اخترت له هذا الموقع لأن ما عالجته فيه من تقنيات تعالج الكثير من المشاكل التي أثرتها في الفصول العشرة السابقة عليه، فقد خصصته لجدران الحماية التي تحمي الشبكات الداخلية من أخطار الإنترنت ومن أخطار الاقتحام والتلصص ومن الفيروسات وغير ذلك. ولما كانت التقنية هي وراء ازدهار جرائم نظم المعلومات وهي أيضًا وراء وسائل المكافحة الناجحة فقد انفردت بالفصل الثاني عشر، بينما خصصت الفصل الثالث عشر لوسائل الإعلام التي أظن أن لها دورًا كبيرًا في توعية العامة في مجال أمن المعلومات، فالإعلام هو العصا السحرية التي نتمنى دائمًا أن تكون في اليد المناسبة. وكان لابد أن نلقي نظرة على الفراغ التشريعي الحالي الذي لا يحاصر هذا النوع من الجرائم كما ينبغي، وعن التشريع في بعض الدول المتقدمة وذلك من خلال الفصل الرابع عشر «التشريع وتجريم جرائم نظم المعلومات». ورأيت أن أختتم البحث بموضوع في غاية الأهمية وهو عن «التحقيق في جرائم نظم المعلومات»، حيث يعالج الفصل الخامس عشر والأخير الكثير من الملاحظات التي تفيد من يتصدى للتحقيق في هذا النوع من الجرائم.

وفي النهاية أتمنى أن يكون في هذا العمل الفائدة المرجوة، وأن يضعه المولى سبحانه وتعالى في ميزان حسناتي.

الفصل الأول

عصر المعلومات

١ . ١ سلاح المعلومات .

١ . ٢ نظم المعلومات .

١ . ٣ المعلوماتية قوة .

١ . ٤ ثورة الاتصالات والإنترنت .

١ . ٥ حرب المعلومات .

عصر المعلومات

يمثل هذا الفصل مقدمة ضرورية لهذا الكتاب إذ أنه يتحدث عن المعلومات كسلاح خطير في هذا العصر، ثم يبين «القيمة المضافة» التي أضافها ظهور الحاسب الآلي إلى المعلومات، ويظهر كيف منحت المعلومات الدول العظمى قوة جديدة، ويتطرق هذا الفصل بعد ذلك إلى ثورة الاتصالات والإنترنت وكيف فتحت آفاقًا جديدة لم تكن متاحة من قبل، ويختتم الفصل بالتوقعات العالمية التي تتنبأ بأن الحرب القادمة ستكون حرب معلومات في المقام الأول.

١ . ١ سلاح المعلومات

يحلو للكثير منا أن يطلق على عصرنا هذا اسم «عصر المعلومات» نظرًا لما اكتسبته المعلومات فيه من أهمية فائقة، ولما أصبح لها من تأثير هائل في البشر والحكومات. فأصبحت المعلومة قوة لا يستهان بها في يد الفرد أو في يد الدولة، بل أصبحت المعلومة سلاحًا في يد المجرمين، ومن هنا نشأ ما نطلق عليه «جرائم نظم المعلومات» وهو موضوع هذا الكتاب.

«وقد أصبحت المعلومات هي المقياس الذي نقيس به قوة الشعوب، فمن يملك المعلومات في هذا العصر وكانت لديه القدرة على حمايتها يستطيع أن يسيطر.. هكذا باختصار شديد. فالسيطرة لم تعد جيوشًا تغزو أو أساطيل تدك المدن أو عسكراً يجوبون شوارع الدول المحتلة، هذا النموذج من السيطرة لم يعد موجودًا هذه الأيام، فقد شهدت حقبة الستينيات من هذا القرن زوال آخر مظاهر هذا النموذج من السيطرة الاستعمارية في العالم» (داود، ٢٠٠٠).

لم يحدث ذلك لاقتناع الدول العظمى، أو الدول الاستعمارية إذا أردنا أن نسمي الأشياء بمسماها الصحيح، لم يحدث ذلك لاقتناع هذه الدول بأن الاستعمار والسيطرة على مقدرات الشعوب الضعيفة هو ضرب من التصرفات غير الإنسانية. ولم يحدث ذلك لضراوة كفاح الشعوب المستعمرة أو لأنها أجبرت الدول الاستعمارية على التقهقر والانسحاب. لا أعتقد أن ذلك كان هو السبب وراء انحسار الموجة الاستعمارية التي غمرت العالم في القرن التاسع عشر والنصف الأول من القرن العشرين. حقيقة الأمر أن الدول ذات الحول والطول اكتشفت وسائل أخرى للسيطرة تتلاءم مع الزمن، كانت هذه الدول تعرف جيدًا أن الهدف الوحيد من وراء الاستعمار كان هدفًا اقتصاديًا بحتًا تكون فيه الدول المستعمَرة مصدرًا للمواد الخام والثروات الطبيعية والعمالة الرخيصة للدول الاستعمارية، في الوقت نفسه تكون المستعمرات سوقًا رائجة لمنتجات مصانع هذه الدول أو ما تفرزه الحضارة الصناعية الضخمة أو الآلة الصناعية الهائلة التي تدور في هذه الدول ووقودها الحقيقي هو هذه المستعمرات. فإذا كان من الممكن للدول الاستعمارية تحقيق الهدف ذاته بأسلوب آخر أكثر حضارة وأقل كلفة وأكثر تمشيًا مع الزمن وبقدر أقل من دماء أبنائها الغالية فلم لا!.

من هنا تحول الاستعمار بأشكاله الفجة إلى الاستعمار الاقتصادي حيث تتحقق نفس الأهداف: تظل المواد الخام والثروات الطبيعية مستنزفة ولكن ليس بالقهر أو الاغتصاب وإنما باستخدام القفازات الحريرية عن طريق الشراء بأسعار السوق، تلك السوق التي يتم توجيهها وتحجيمها والسيطرة عليها بشكل أو آخر، والعمالة الرخيصة كذلك أمكن تأمينها ولكن في صورة مختلفة فيما نطلق عليه الآن العقول المهاجرة، فهذه الدول تستقطب العقول الفذة لدى الشعوب النامية، تلك العقول التي كان من الممكن أن تصنع

لبلادها نهضة اقتصادية أو نهضة علمية أو ثقافية، تذهب هذه العقول الآن طائعة راضية مختارة إلى الدول الكبرى بمحض إرادتها لتزيد القويَّ قوة وتزيد الغنيَّ غنى، وتخصم في الوقت نفسه من رصيد بلادها وتُهدر الملايين التي أنفقتها بلادهم على تعليمهم وتدريبهم وإعدادهم ليكونوا في النهاية تروسًا في عجلة الاقتصاد الضخمة في الدول الكبرى فتزداد بذلك الهوة بين الغني والفقير وتتسع الفجوة التقنية والفجوة الاقتصادية والفجوة الحضارية في نهاية الأمر.

واستخدام الدول النامية كسوق مازال قائمًا، ولكن دون ضغط أو إرغام، فبدلاً مما كانت تفعله الدول الاستعمارية في الماضي من احتكار لهذه الأسواق وفرض لبضائعها فيها عن طريق سن ضرائب ورسوم باهظة على منتجات الدول الأخرى، بل أحيانًا على منتجات الشعب المحتل نفسه، بدلاً من ذلك نجدها الآن تقدم بضاعتها مدعومة بقروض تشترط على الدول النامية أن تشتري بها منتجات الدول الغنية، وأن تنقل هذه الواردات باستخدام ناقلات هذه الدول أو أن يتم التدريب على استخدامها من خلال مؤسسات هذه الدول الغنية. ونرى كيف أن الدول الكبرى تربط بعقود التسليح الكثير من العقود الأخرى، وعقود التسليح تلك هي العقود التي كثيرًا ما نرى الدول النامية تسعى بنفسها إلى إبرامها والحرص على تكديس الأسلحة نتيجة التسخين المستمر للأحداث والأوضاع في المناطق التي تعيش فيها هذه الدول. فنجد في هذا العصر جارات شقيقات تتحارب أو تغزو إحداهما الأخرى، ونرى في الدولة الواحدة فرقًا تتصارع، والسبب ليس مهمًا، فقد يكون دينيًا أو مذهبيًا وقد يكون عرقيًا أو أيديولوجيًا.. لا يهم السبب ولكن المهم أن يظل الصراع ساخنًا وأن تظل الحاجة إلى السلاح قائمة. وقبل ذلك وأهم من ذلك أن تظل الحاجة إلى حماية الدولة

الاستعمارية قائمة، بل تأتي هذه الدول التي صنعت المشكلة، وبكل مهارة، لتؤدي دور وسيط السلام الذي يطفئ النار التي أشعلتها بنفسها، وذلك حتى لا يأتي طرف آخر يطفئ هذه النار خشية أن تفقد ما لها من نفوذ وما لها من سيطرة على السيناريو الموضوع، وتمنع هذه الدول جاهدة أية جهة أخرى تحاول القيام بهذا الدور حتى تشتد الحاجة إليها وتظل منفردة في بؤرة الصراع فيصبح في مقدورها، وهذا هو الأهم، إعادة إشعال النار من جديد إذا دعت الحاجة إلى ذلك. أي أن الاستعمار الآن قد خلع عباءته العسكرية وارتدى عباءة اقتصادية.

١ . ٢ نظم المعلومات

صادف أن ترافق هذا التحول التكتيكي في الفكر الاستراتيجي الاستعماري مع تحول ضخم آخر غير الخريطة العلمية للعالم وقلب جميع الموازين وخلط كافة الأوراق وهو اختراع الحاسب الآلي... فقد ساعد هذا الاختراع، الذي يمكن القول إنه يماثل اختراع الكهرباء في العصر الحديث أو اختراع النار في عصور ما قبل التاريخ، أقول أن هذا الاختراع ساعد على تحقيق شيئين اثنين أو كانت له قيمتان اثنتان هما : القدرة الضخمة على تخزين المعلومات واسترجاعها عند الحاجة، والسرعة الهائلة التي تمكن من التعامل مع هذه المعلومات والربط بينها واستخلاص المفيد منها، وما استتبع ذلك من قدرات متنامية على استنتاج ما تشير إليه هذه المعلومات من حقائق، هذه الحقائق التي تكون في العادة خافية على متخذ القرار في غيبة تلك المعلومات ولا تظهر إلا من خلال معالجة المعلومات المتوفرة وعرضها في الصورة الملائمة (داود، ٢٠٠٠).

وهكذا أدى ظهور الحاسب الآلي إلى ارتفاع قيمة المعلومات، إذ أنه يُكسب المعلومات (قيمة مضافة)، لأنه بدون قدرات الحاسب الهائلة لا تكون للمعلومات نفس القيمة، فالفائدة المرجوة من المعلومات غير المرتبة أو غير المخزنة أو غير القابلة للربط والاستخلاص لهي فائدة محدودة. وبارتفاع قيمة المعلومات وأهميتها وتزايد القدرة على استخدامها أصبحت تُوظف بذكاء للاستفادة منها اقتصاديًا، وأصبح الحاسب والمعلومات معًا في خدمة الاقتصاد. وكان من الطبيعي بعد ذلك أن تكتسب أهمية المعلومات بعدًا عسكريًا وسياسيًا. ولما كانت الدول الكبرى هي دائمًا السباقة للاختراع والسباقة لجني الثمار فإنها كانت السباقة كذلك لتثمين هذا العامل الجديد وتقدير أهمية المعلومات وخطورتها ومن ثم توظيفها والاستفادة منها. أصبحت المعلومات إذن السلاح الجديد الذي تحارب به الدول العظمى، وما كان ذلك ليتحقق دون وجود تلك الأداة الخطيرة التي تمكن من الاستفادة من المعلومات وأعني بها الحاسب الآلي.

شيئًا فشيئًا أصبح الحاسب الآلي نفسه أداة هامة من أدوات الحرب (حرب الاقتصاد وحرب الإعلام وحرب السيطرة) خاصة بعد أن تغلغل الحاسب الآلي في كل المجالات بسلاحيه الهائلين : القدرة الفائقة على تخزين المعلومات، والسرعة الهائلة في التعامل مع هذه المعلومات. ولذلك رأينا خلال العقدين الأخيرين اللذين يطوي بهما العالم الصفحة الأخيرة من الألفية الميلادية الثانية ليستقبل ألفية جديدة ثالثة، رأينا خلال هذين العقدين كيف أن علوم الحاسب قد ركزت على هذين المجالين : القدرة على التخزين وسرعة المعالجة، ولا تمر سنة (أقول سنة بكثير من التحفظ فهي قد تكون أقل من ذلك بكثير) دون أن يصل العلم إلى سعة تخزين أكبر وسرعات أعلى دون أن يبدو في الأفق سقف تصل إليه هذه المنجزات أ

يتوقف عنده تطور التقنيات. ونرى هؤلاء الذين يطورون تلك التطبيقات التي تستفيد من إمكانيات الحاسب الآلي يلهثون باستمرار وراء تلك التقنيات للاستفادة منها.

ويظل الحاسب الآلي دائمًا هو ذلك السلاح الأقوى في عصر المعلومات وتلك الأداة التي لا غنى عنها. ولم تغب هذه الحقيقة عن الدول الكبرى، فنرى هذه الدول ترفض بيع أجهزة الكمبيوتر المتطورة لديها مثل السوبر كمبيوتر إلى الدول (غير الصديقة)، أو الدول التي تُخشى منافستها إما في سوق الاقتصاد أو في سوق السياسة، أو الدول التي يُظن أن لديها برامج للتسليح النووي، ذلك لأن الحاسبات المتطورة تسرع كثيرًا من معدل التقدم في هذه البرامج وتساعد على تنفيذها.

وهذا الاهتمام بالحاسب الآلي وعلومه واستخداماته لم يعد خافيًا على الدول العربية بصفة عامة فوجدنا خلال العقد الأخير من القرن العشرين كيف انتشر تدريس الحاسب في المدارس حيث بدأ دخوله في المدارس الثانوية ثم توسع استخدامه حتى أصبح مادة تدرس في المدارس الابتدائية ومراحل التعليم ما قبل الأساسي، وفي كثير من الدول العربية أصبحت مادة الحاسب الآلي تدرس ضمن مناهج جميع الكليات بلا استثناء، حيث استقرت في الأذهان ضرورة إتقان استخدام الحاسب الآلي بواسطة المتخصصين في أي مجال فلا يُستغنى عن استخدامه في مجالات كالطب والزراعة والصناعة والتعليم والصحافة وغيرها. وهكذا، كما ذكرنا، فالحاسب الآلي أصبح أداة هامة من أدوات الحرب والسلام في نفس الوقت وعلى نفس الدرجة من الأهمية في كل حالة منهما.

١ . ٣ المعلوماتية قوة

شيئًا فشيئًا نرى الدول الاستعمارية تخلع العباءة الاقتصادية السافرة لتستخدم عباءة جديدة أكثر خطورة وأكثر جدوى نسجتها من هذا السلاح الجديد سلاح المعلومات . وشيئًا فشيئًا أخذ يتشكل ما يمكن أن نطلق عليه عصر المعلومات، أو عصر المعلوماتية إذا أردنا أن نختار تعبيرًا أكثر شمولاً إذ هو يضيف إلى المعلومات نفسها تلك الأدوات التي تعالج هذه المعلومات وتستفيد منها. هذه الأدوات منها الحاسبات والأجهزة والتقنيات والبرامج التي تخدمها، كما أنه يضيف كذلك البيئة التي تستخدم هذه المعلومات بل والبشر الذين يقومون على خدمتها وإعدادها وتفعيلها .

المعلوماتية إذن هي السلاح النووي الجديد الذي قد يفصل بين النصر والهزيمة في حالة الحرب، فمن يعلم سوف ينتصر حتى لو لم يكن هو الأقوى، ومن لا يعلم سوف ينهزم حتى لو كان هو الأقوى (داود، ٢٠٠٠) . إذ قال الله تعالى ﴿قُلْ هَلْ يَسْتَوِي الَّذِينَ يَعْلَمُونَ وَالَّذِينَ لاَ يَعْلَمُونَ﴾ (الزمر، ٩) .

وفي زمن السلام نجد أن المعلومات أيضًا هي القوة الهائلة والأصل الثمين من أصول أي مؤسسة أو دولة، ونجد أن هذه الدول وتلك المؤسسات تنفق الكثير على معلوماتها، سواء لحفظها أو تأمينها أو لتطوير أساليب أفضل للاستفادة منها، ذلك لعلم الجميع بأهمية المعلومة وأهمية وصولها إلى الطرف المطلوب في الوقت المناسب، فإذا توفرت معلومات معينة مثلاً لفريق كرة القدم عن الفريق المنافس قبل المباراة فإن ذلك قد يكون سببًا في النصر .

١ . ٤ ثورة الاتصالات والإنترنت

بازدياد حجم المعلومات وكثافتها ازدادت الحاجة إلى تبادلها وإلى انتقالها من مكان إلى آخر، إما داخل المؤسسة الواحدة أو من مؤسسة إلى أخرى أو حتى بين الدول. وهكذا ظهر ما أطلقنا عليه ثورة الاتصالات وأخذ هذا الفرع من فروع الهندسة ينمو ويلتقي ويتقاطع مع علوم الحاسب حتى ظهرت شبكات المعلومات ووجدنا كيف أنها انتشرت وبسرعة مذهلة في كل مكان وامتدت كابلاتها وخطوطها تنقل كميات هائلة من المعلومات عبر الكرة الأرضية، وانطلقت أقمار اصطناعية عديدة تحيط بالأرض من كل جانب لتسهل انتقال المعلومات دون الحاجة إلى مرورها في الكابلات أو بين أطباق الميكروويف (داود، ٢٠٠٠).

وأخيرًا جاءت شبكة إنترنت لتضع المعلومات على اختلاف أنواعها وكمياتها وأهدافها عند أنامل الجميع، فأصبح كل فرد الآن يستطيع عن طريق هذه الشبكة، التي يستخدمها الملايين، أن يحصل على ما يشاء من معلومات من مختلف أنحاء الدنيا في أي لحظة من ليل أو نهار، فعلى مدار الساعة تدور هذه الطاحونة الهائلة (إنترنت) بلا توقف لتصل بين البشر جاعلة من العالم قرية صغيرة. وظهور هذه الشبكة العالمية الساحرة سوف يقلب الموازين مرة أخرى وسوف يجعل الجميع يعيدون حساباتهم من جديد، أقوياء وضعفاء. . . مستعمِرون ومستعمَرون بعد أن تبين ما لها من فوائد هائلة ومن عيوب خطيرة.

١ . ٥ حرب المعلومات

في يناير ١٩٩٧ أصدرت وزارة الدفاع الأمريكية تقريرًا خطيرًا يؤكد على الحاجة لجهود غير عادية تتطلبها الممارسات الحالية، التي إذا تُركت

لتستفحل فسوف تؤدي حتمًا لكارثة أمنية قومية، ويحذر التقرير من «بيرل هاربور إلكترونية» في تلميح واضح إلى حادث الهجوم المفاجئ لسلاح الجو الياباني خلال الحرب العالمية الثانية على الأسطول الأمريكي في ميناء «بيرل هاربور». يتوقع هذا التقرير أن يزداد الهجوم على نظم المعلومات في الولايات المتحدة بواسطة جماعات إرهابية أو عصابات الجريمة المنظمة أو عملاء المخابرات الأجنبية، وأن يصل هذا الهجوم إلى ذروته في العام ٢٠٠٥. ويوصي التقرير باعتماد ميزانية إضافية قدرها ثلاثة مليارات دولار ليتم إنفاقها خلال السنوات الخمس من عام ١٩٩٧ إلى عام ٢٠٠١ لتحسين الوضع الأمني لشبكة الاتصالات والبنية التحتية لاستخدامات الحاسب الآلي في الولايات المتحدة. كما أوضح التقرير أن الجيش الأمريكي بما يحتويه من ١,٢ مليون جهاز حاسب وعشرة آلاف شبكة محلية معرض بشدة للاختراق. وينتقد التقرير بعنف الجهود الأمنية الحالية للبنتاجون ويصفها بعدم الكفاية ويحث على بدء استخدام نظام إنذار ذي خمس مستويات يستطيع، عند اكتشاف أي هجوم، تأمين مراقبة لصيقة لنظم المعلومات الحساسة (المتعلقة بالأمن القومي الأمريكي) ثم يقوم بفصلها عن نظم المعلومات الخارجية. ووصل هذا التقرير الذي نشرته الصحف في الولايات المتحدة في نفس يوم صدوره ونقلته عنها وكالات الأنباء العربية أن شبكة الاتصالات ومصادر الطاقة الكهربية والبنوك وصناعات النقل في الولايات المتحدة معرضة جميعها للهجوم من جانب أي جهة تسعى لمحاربة الولايات المتحدة دون أن تواجه قواتها المسلحة. ويدعو التقرير إلى زيادة الإنفاق على البحث العلمي، خاصة من جانب القطاع الخاص، بهدف تطوير برامج وأجهزة جديدة لتوفير الأمن، بما في ذلك تطوير نظام آلي لتعقب المقتحمين لتحديد هويتهم.

الفصل الثاني

جريمة نظم المعلومات

٢ . ١ جريمة نظم المعلومات؟

٢ . ٢ بعض مصطلحات جرائم نظم المعلومات .

٢ . ٣ المعلومات المطلوب حمايتها .

٢ . ٤ سرية المعلومات .

٢ . ٥ جرائم نظم المعلومات في التاريخ .

٢ . ٦ مستقبل جرائم نظم المعلومات .

جريمة نظم المعلومات

نحاول في هذا الفصل أن نجد تعريفًا مناسبًا لجريمة نظم المعلومات ولبعض المصطلحات الأخرى المتداولة في مجال جرائم نظم المعلومات. نحاول بعد ذلك توضيح نوعية المعلومات المطلوب حمايتها، ثم نناقش قضية هامة وهي: هل نطبق قاعدة أن «الأصل في الأشياء الإباحة» أم نطبق قاعدة «المعرفة على قدر الحاجة». ونقدم بعد ذلك قصة أكبر جرائم نظم المعلومات في التاريخ لكي نبين خطورة هذا النوع من الجرائم والمدى الذي يمكن أن تصل إليه. ونختتم الفصل بالحديث عن مستقبل جرائم نظم المعلومات، وما يحمله المستقبل من أنواع جديدة من هذه الجرائم، خاصة مع دخول الكمبيوتر الذكي إلى منزل المستقبل وإلى الأجهزة المنزلية.

٢ . ١ جريمة نظم المعلومات؟

إذا قبلنا تعريف الجريمة باعتبار أنها «أي سلوك سيئ متعمد يتسبب في إلحاق الضرر بالضحية (أو يعرض الضحية إلى ضرر محتمل)، أو ينتج عنه حصول الجاني (أو محاولته الحصول) على كسب أو فائدة لا يستحقها»، فلكي نعرف جريمة نظم المعلومات فيجب أن نضيف إلى هذا التعريف شرط أن تتضمن الجريمة «إتلاف المعلومات أو إساءة استخدامها». واشتراط أن يكون ذلك عن طريق استخدام نظم المعلومات، أي يصبح تعريف جريمة نظم المعلومات على النحو التالي:

«جريمة نظم المعلومات هي السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها، مما يتسبب (أو يحاول التسبب) إما في إلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها».

٢ . ٢ بعض مصطلحات جرائم نظم المعلومات

نقدم فيما يلي بعض المصطلحات التي سوف يصادفها القارئ في هذا الكتاب والتي يكثر تداولها عند تناول موضوع جرائم نظم المعلومات :

قرصنة البرامج: حيازة أو استخدام برامج الحاسب بدون ترخيص من المالك .

حصان طروادة: زرع بعض الأوامر خلسة في برنامج ، أو إضافة دوائر إلكترونية خلسة في بعض قطع الحاسب وأجهزته .

الفيروس: برنامج يعد خصيصًا ليتم إقحامه خفية في أحد برامج الكمبيوتر ، ومن خصائصه أن تكون لديه القدرة على مضاعفة نفسه وعلى أن ينسخ نفسه في برامج أخرى عند تشغيله في الحاسبات .

المتسلل: (Hacker) أحد المغرمين بالحاسب والبارعين في علومه ، والذي لديه الفضول لاكتشاف ما تحتويه حاسبات الآخرين ، ولكنه يقوم بذلك عن طريق استخدام وسائل غير مشروعة .

وجدير بالذكر أن كلاً من «ستيفن ليفي» (Levy,1984) و«بروس ستيرلنج» (Sterling,1996) قد أعطياه التعريف المختصر التالي : (مدمن الكمبيوتر الذي يجد لذته في الوصول إلى البيانات الممنوعة) . ولكننا نفضل التعريف الذي اخترناه لأنه أكثر دقة .

المقتحم: مجرم يتورط في عمليات التسلل إلى نظم الحاسب لإلحاق الضرر بالمعلومات المخزنة فيه أو سرقتها ، أو هو مقتحم يعمد خلسة إلى نشر الفيروسات على ضحاياه الأبرياء .

جريمة الإنترنت: هي جريمة يرتكبها المجرم من خلال شبكة الإنترنت .

٢ . ٣ المعلومات المطلوب حمايتها

في محاولة للإجابة عن السؤال الصعب الخاص بنوعية المعلومات المطلوب حمايتها نذكر هذه الأنواع من المعلومات:

٢ . ٣ . ١ الأسرار الداخلية للشركات

والمقصود بها تلك الأسرار التي قد يؤثر إفشاؤها على مكانة هذه الشركات أو موقفها في السوق. ويشكل الصحفيون والشركات المنافسة مصدر الخطر الرئيسي على هذا النوع من المعلومات، فهم مهتمون بصفة خاصة بحجم الأعمال أو بقائمة العملاء مثلاً. وفي بعض الأحيان يكون موظفو الشركة أنفسهم مصدر تسرب المعلومات، ففي إحدى شركات صناعة الكمبيوتر الكبرى شكا مهندسو النظم من (سفينتهم الغريبة التي يتسرب الماء من أعلاها!) وهم بذلك يقصدون أن كبار الموظفين يثرثرون قبل الأوان عن خطط الشركة الإنتاجية.

٢ . ٣ . ٢ المعلومات المالية

يحتاج رجال الأعمال إلى التأكد من أن المعلومات المالية، خاصة تلك المعلومات التي يتم نشرها على نطاق واسع، هي معلومات كاملة ودقيقة، ولذلك نجدهم يعتنون بتنفيذ إجراءات التحقق من سلامة هذه المعلومات بشكل دوري، وكذلك بتحديثها على فترات محددة. وبدأ الاتجاه الآن بين كثير من الشركات في العالم وفي المنطقة العربية أيضًا لاستخدام شبكة الإنترنت العالمية أو شبكات الإنترانت الداخلية لضمان سرعة نشر هذه المعلومات على نطاق واسع. كما يستخدمون هذه الشبكات كذلك لتحديث هذه المعلومات المالية حتى تكون دائمًا سليمة وفي أحدث صورة لضمان اتخاذ القرار السليم في الوقت المناسب.

٢ . ٣ . ٣ الأسرار التجارية

برغم أنه توجد الآن درجة عالية من الشفافية في أعمال الشركات إلا أن هناك بعض الأسرار التجارية التي تود الشركات ألا تتسرب . ولعل من الأمثلة الشهيرة على هذا النوع من الأسرار التركيبة السرية لشركة (كوكاكولا) أو ربما الخلطة السرية لدجاج «كنتاكي» . ولقد صدر مؤخرًا في الولايات المتحدة تشريع يجرم سرقة الأسرار التجارية للشركات ويعتبرها جريمة فيدرالية . ومن الوسائل الشائعة الاستخدام لسرقة هذه الأسرار استخدام أسلوب « الهندسة العكسية» (Reverse Engineering) للحصول على أسرار المنتجات، أو رشوة واستمالة موظفي الشركة المنافسة لإفشاء هذه الأسرار . ولكن القوانين الحالية لا تعتبر هذه الأعمال أعمالاً إجرامية إلا إذا توفر سوء النية لدى مرتكبها وأثبتت الضحية أن هناك ضررًا فعليًا قد وقع عليه .

٢ . ٣ . ٤ المعلومات التقنية

نقصد بها المعلومات الفنية المستخدمة في الإنتاج ، فبعض الشركات لا تهتم أحيانًا بتوثيق الخطوات العديدة التي يتطلبها إنتاج وتوزيع منتجاتها أو خدماتها . وبدلاً من ذلك يحتفظ بعض الموظفين الأساسيين بهذه المعلومات في رؤوسهم ، ويتطلب الأمر أن تشجع الشركات هؤلاء الموظفين على توثيق معلوماتهم ومن ثم اتباع إجراءات أمنية جديدة للتأكد من أن هذه المعلومات يتم الاحتفاظ بها في مكان آمن ويتم تحديثها كلما لزم الأمر .

٢ . ٣ . ٥ المعلومات عن الموارد البشرية

عند تعامل المؤسسات مع بيانات موظفيها التي تحتفظ بها تثور دائمًا مشكلة الخصوصية ، فالشركات تحتاج للعناية الخاصة بحماية الملفات التي

تحتوي على معلومات الموظفين وبياناتهم الشخصية ومنها المرتبات والمعاشات وبيانات التأمين عليهم والحالة الصحية وتقارير الأداء وغير ذلك. وفي هذه الأيام تسمح الكثير من الشركات لموظفيها بالاطلاع على أجزاء كثيرة من سجلاتهم الشخصية المحفوظة في الحاسب بل وتعديلها بأنفسهم على اعتبار أن ذلك يزيد من درجة صحة هذه المعلومات وتكاملها برغم أن هذا الأمر يزيد من درجة تعرض هذه السجلات للخطر.

٢ . ٣ . ٦ معلومات العملاء

تحتاج الشركات دائمًا للاحتفاظ بمعلومات مفصلة عن عملائها وطبيعة عملهم، فمثلاً بالنسبة لشركة تورد رقائق السليكون لعميل يقوم بصنع المعالجات الدقيقة للحاسب، قد تحتاج هذه الشركة لمعرفة بعض التفاصيل المتعلقة بإنتاج هذا العميل ومكونات المنتج ومراحل الإنتاج. وبعض هذه المعلومات قد يكون حساسًا، والشركات التي تريد تثبيت أقدامها في السوق عليها إثبات قدرتها على الاحتفاظ بسرية مثل هذه المعلومات التي تخص عملاءها، على نفس المستوى الذي تحتفظ فيه بسرية المعلومات الأخرى الخاصة بها كبيانات مسح السوق مثلاً.

٢ . ٣ . ٧ سلعة المعلومات

الكتب والبرمجيات والتسجيلات الصوتية والأفلام والخرائط والإعلانات وغيرها من السلع التي تدخل المعلومات في تكوينها بنسبة كبيرة تتم حمايتها بواسطة قوانين حقوق الملكية الفكرية، والقانون يحمي حقوق استخدام هذه الأعمال في مختلف صورها وعلى مختلف الوسائط التي قد تنقل إليها، ولكن هذه الحماية موقوتة بفترة زمنية محددة، وتم منذ فترة قريبة تعديل القانون الأمريكي ليتضمن النص على حماية برامج الكمبيوتر

سواء في صورتها الأصلية (source) أو المترجمة (object). ومثلما يلجأ منتجو الخرائط إلى إضافة بعض العلامات السرية أو المائية الخاصة في خرائطهم لتمكنهم من كشف التزييف، فالمبرمجون أيضًا يقومون بالشيء نفسه لحماية برامجهم. وتقوم شركات البرمجة باستخدام علامات سرية ضمن العلامة التجارية للشركة (Logo) كما تستخدم وسائل حديثة لإضافة «العلامات المائية الرقمية» (Digital Watermarking) لإثبات حقوق الملكية، وعند نسخ البرنامج بصورة غير قانونية يتسبب وجود العلامة المائية في إزاحة بعض الكلمات المعينة أو بعض السطور في النص بمقدار أجزاء من المليمتر بحيث يمكن تمييز الوثيقة الأصلية من المنسوخة، وكذلك على شاشة الحاسب تتم إزاحة بعض الكلمات بمقدار «بيكسل» واحد فقط ولكنه يكون كافيًا لكشف التزوير دون أن تلحظه عين غير خبيرة.

٢ . ٣ . ٨ المعلومات المؤقتة

هناك الكثير من المعلومات ذات الطبيعة المرحلية أو المؤقتة مثل الخطابات اليومية التي يتم تبادلها داخل الشركة أو المذكرات أو مسودات التقارير وتسجيلات المحادثات. هذه المعلومات قد تكون لها قيمة استراتيجية للمؤسسة أو الشركة، ومن الصعب تحديد درجة سرية معينة لمثل هذه المعلومات أو تصميم إجراءات حماية أمنية لها. إلا أنه من الضروري أن تضع المؤسسة أهمية هذا النوع من المعلومات في الاعتبار وتنبيه الموظفين لهذه الأهمية.

٢ . ٣ . ٩ المعلومات الأمنية

«أمن الأمن» إذا جاز هذا التعبير، لا يلقى في العادة الاهتمام الكافي، فالمعلومات التفصيلية حول كيفية حماية المعلومات الاستراتيجية في المؤسسة

تكون لها أهمية خاصة وحساسية عالية لأنه من الممكن أن يساء استخدامها بصورة أو بأخرى.

وللأسف من خلال لقاءاتي مع العديد من مسئولي أمن المعلومات لاحظت أنهم يقومون بإفشاء الكثير من التفاصيل حول وسائل تأمين مؤسساتهم أو حول نقاط الضعف الأمنية لديهم، ولعل هذا الأمر يشكل انتهاكًا أمنيًا كبيرًا من المهم تداركه.

٢ . ٤ سرية المعلومات

المطلوب من مديري الشركات أن تكون لديهم معرفة كاملة عن كل شيء من المنتجات أو الخدمات التي تقدمها شركاتهم، وموارد وإمكانيات الشركة، بل ويجب أن تكون لديهم معرفة كاملة بالشركات المنافسة. هذه المعارف يجب أن تتم معالجتها واستخدامها بشكل متطور حتى تكون ذات فائدة، ومن هنا جاء مصطلح «إدارة المعرفة» أو (Knowledge Management) وهو مفهوم جديد ظهر مع ظهور مفهوم «إدارة الجودة الكلية» أو (Total Quality Management) ويفرض علينا هذا الاتجاه الجديد أن نعيد التفكير في بعض أوجه أمن المعلومات. ويعرف هذا المفهوم «آلان كانترو» مسئول المعارف في شركة «مونيتور» الاستشارية (Kantrow,1999) على النحو التالي (تتكون هذه النظرية من تجميع المعارف التي يتم الحصول عليها بواسطة الأفراد ونشرها بين الآخرين في المؤسسة) بينما يدعو «دوجلاس كال» المدير الإقليمي لخدمات أمن الحاسب بشركة «دلويت آند توتش» (Cale,1999) إلى التركيز على الحاجة إلى تبسيط نظم السرية وإلى إتاحة المعلومات للجميع بقدر الإمكان، وذكر «كال» كيف قامت إحدى المؤسسات الكبرى في الولايات المتحدة بالفعل بتبسيط درجات السرية لديها

من خمسة مستويات إلى مستويين فقط تطبيقًا لمنطق إتاحة كل المعلومات لجميع الأفراد بالمؤسسة باستثناء جزء بسيط من المعلومات التي يجب أن تظل ذات طابع سري (أي أن الأصل هنا هو الإباحة والاستثناء هو الحظر)، وذلك تطبيقًا للمبدأ المستعار من الشريعة وهو «الأصل في الأشياء الإباحة». ولكن يتناقض هذا المبدأ مع قاعدة «المعرفة على قدر الحاجة» التي تقضي بحظر كل المعلومات عن الجميع فيما عدا ذلك الجزء البسيط الذي لا يستغني عنه الفرد حتى يتمكن من أداء عمله. هذا المبدأ في ظني يعتبر حيويًا في الجهات العسكرية أو الجهات ذات الطابع الأمني الصرف التي يكون الهدف الأهم فيها هو تحقيق الأمن بأي ثمن، إلا أنه لا يصلح في الشركات التي تهدف دائمًا إلى الربح وزيادة الإنتاج وتحقيق النمو بأقل تكلفة.

ولكن ما هي المعلومات التي يجب تأمينها وحمايتها؟ وهل يتضمن التأمين عدم الاطلاع على المعلومة بالمرة أم يمكن السماح بالاطلاع عليها ولكن مع عدم السماح بتعديلها؟ الإجابة عن هذين السؤالين صعبة للغاية، ولعل في القصة التالية ما يدل على أن هناك بعض المعلومات التي قد تبدو بسيطة وليست في حاجة للتأمين، بينما هي في الحقيقة ليست كذلك.

في الوحدة الدولية لأبحاث الفيزياء النووية بسويسرا، قام أحد المتسللين (hackers) منذ عدة سنوات بالدخول إلى الحاسب الرئيسي بالوحدة وقام - على سبيل المزاح - بتغيير رقم واحد في قيمة النسبة التقريبية «ط» (π) والتي تساوي ١٤٢٨٥٧, ٣حيث جعلها ١٤٣٨٥٧, ٣، وقد نتج عن هذا التغيير البسيط الذي لم يلحظه الباحثون خسارة ملايين الدولارات بسبب النتائج الخاطئة للأبحاث، لأن الحاسب الآلي استخدم المساحة الخطأ والمحيط الخطأ للدوائر في حساباته، حيث يدخل هذا الرمز في الكثير من الحسابات.

٢ . ٥ جرائم نظم المعلومات في التاريخ

لا يستطيع أحد أن يدعي أنه من الممكن تحديد أكبر جرائم الحاسب، لسبب بسيط وهو أن هذا النوع من الجرائم لا يعلن منه إلا القليل، ولكننا نستطيع أن نورد هنا أكبر جرائم الحاسب (المعلنة)، ولعل أكبر هذه الجرائم على الإطلاق، سواء في حجمها أو في حجم الخسائر الناجمة عنها، هي جريمة «لوس أنجلوس» التي وقعت في عام ١٩٧٣ والتي أدت إلى تدمير أكبر شركات التأمين على الاستثمارات المالية «إكويتي فندنج إنشورنس» (EFI) وبلغت الخسائر فيها مليارين من الدولارات (Seidler,1977) . فقد أرادت الإدارة الجديدة التي تولت أمر الشركة أن تجعل منها أسرع الشركات نموًا وأن تصبح أكبر شركة على الإطلاق في صناعة التأمين . ولكن للأسف حاولت الشركة الوصول إلى هذه النتيجة عن طريق التورط في جميع أنواع الاحتيال والخداع المعروفة (وغير المعروفة)، ومن خلال تورطهم وترديهم السريع في متاهات الجريمة اختلقت الشركة ٦٤ ألف شخص وهمي وسجلتهم في الحاسب الخاص بالشركة على أنهم عملاء لها، وقامت بالتأمين على حياتهم بوثائق تأمين وهمية، ثم باعت هذه الوثائق لشركات إعادة التأمين . وأدانت التحقيقات والمحاكمة التي تلت اكتشاف الجريمة ٢٢ من كبار الموظفين منهم اثنان يعملان في الشركة التي تولت أعمال الرقابة والمراجعة على هذه الشركة !! (Parker,1976) .

وهناك واقعة حديثة نسبيًا، حيث وقعت في عام ١٩٩٥، وتداولتها وسائل الإعلام بشكل مكثف في ذلك الوقت . وهي واقعة انهيار بنك «بارينجز» في لندن، فقد قام مندوب البنك في سنغافورة بعدة استثمارات ومضاربات ضخمة في البورصة من خلال بورصة الأوراق المالية في طوكيو . ولكن عندما تأثرت هذه الاستثمارات في أعقاب زلزال «كوبي»

الشهير حاول هذا المندوب إخفاء الخسائر الضخمة باستخدام حسابات جانبية وهمية أدخلها في الحاسبات الخاصة بالبنك، فظهر الأمر وكأن الأموال قد انتقلت من حساب إلى آخر، وساعده بعض متخصصي الحاسب الآلي في ذلك. وقد بلغ إجمالي الخسائر كما ذكرنا في موضع سابق من هذا الفصل حوالي مليار ونصف من الدولارات (Fay,1997).

٢ . ٦ مستقبل جرائم نظم المعلومات

نتوقع أن يحمل المستقبل أنواعًا جديدة غير متوقعة من جرائم نظم المعلومات، وسيحتاج خبراء أمن المعلومات إلى أن يظلوا في حالة استنفار دائمة في مواجهة هذه الأنواع الجديدة، وستظل وسائل الإعلام حريصة على إبراز المثير والغريب من هذه الجرائم. كما نتوقع أن تُستخدم تقنيات حديثة ومتقدمة في هذه الجرائم مثل تقنيات التعرف على الصوت وتقنيات تحديد الشخصية.

مع دخول الكمبيوتر الذكي إلى المنازل وإلى الأجهزة المنزلية فإن ذلك سيفتح الباب لأنواع متطورة من الجرائم التي تستغل إمكانية برمجة الأجهزة المنزلية ووصلها بالحاسب الآلي وبشبكة الإنترنت، فطالما أنك تستطيع مثلاً وصل خزانة الأموال في مكتبك بشبكة الإنترنت لإعطاء إنذار عند محاولة فتحها فربما كان من الممكن فتحها عن بعد بواسطة الكمبيوتر ثم الوصول إليها وإفراغها!

الحرب القادمة الحرب القادمة في الشرق الأوسط، في حال وقوعها، ستكون حرب معلومات بالدرجة الأولى، بمعنى أن أطراف الصراع سيحاولون تحقيق التفوق في مجال المعلوماتية على الأطراف الأخرى. فسيحاول كل طرف تدمير البنية التحتية للمعلوماتية للأطراف

الأخرى من شبكات ومراكز اتصالات. وسيحاول كل طرف إفساد قواعد بيانات الأطراف الأخرى وإتلاف المعلومات المخزنة فيها لما لها من قيمة استراتيجية عظيمة. كما سيحاول كل طرف ممارسة التجسس الإلكتروني والتنصت على الاتصالات المتداولة عبر شبكة الإنترنت، وسيحاول كل طرف ابتكار وسائل أحدث وأكثر فعالية لكسر الشفرة التي يستخدمها الطرف الآخر في حماية معلوماته واتصالاته.

وعلينا أن ننتبه جيدًا إلى أهمية أمن المعلومات وأمن الشبكات والاتصالات، فهذا العلم سيجعل للدولة التي تتمرس فيه اليد الطولى في الحرب القادمة، قال الله تعالى: ﴿وَأَعِدُّواْ لَهُم مَّا اسْتَطَعْتُم مِّن قُوَّةٍ وَمِن رِّبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللهِ وَعَدُوَّكُمْ﴾ (الأنفال، ٦٠).

الفصل الثالث

أنواع جرائم نظم المعلومات

٣ . ١ تصنيف جرائم نظم المعلومات .

٣ . ٢ تخريب المعلومات وإساءة استخدامها .

٣ . ٣ الإهمال .

٣ . ٤ إغفال الواجب .

٣ . ٥ تزوير البيانات .

٣ . ٦ التزييف .

٣ . ٧ الابتزاز .

٣ . ٨ تزوير العلامات التجارية .

٣ . ٩ انتهاك الخصوصية .

أنواع جرائم نظم المعلومات

نحاول في بداية هذا الفصل أن نصنف بعض جرائم نظم المعلومات والوسائل التي تسهل ارتكابها. ثم نتعرض فيما تبقى من الفصل لأنواع مختلفة من جرائم نظم المعلومات. من هذه الجرائم تخريب المعلومات وإساءة استخدامها، والإهمال، وإغفال الواجب، وتزوير البيانات، والتزييف والابتزاز، وانتهاء بتزوير العلامات التجارية. ثم نختتم الفصل بالحديث عن جريمة انتهاك الخصوصية الفردية حيث نفي هذا الموضوع حقه فنتحدث عن حق الحكومات في الاطلاع على المعلومات الشخصية والخاصة للأفراد، ونبين كيف ينظر العالم المتقدم لخصوصية الأفراد وكيف ينظر لها العالم الثالث.

ونظرًا لأهمية الجرائم التي ترتكب من خلال شبكة الإنترنت فإننا سوف نفرد أكثر من فصل لأنواع الجرائم التي ظهرت مع ظهور شبكة الإنترنت وأصبحت لصيقة بها حتى أنها أخذت اسم «جرائم الإنترنت».

٣ . ١ تصنيف جرائم نظم المعلومات

لا تختلف جرائم نظم المعلومات عن الجرائم التي توالى حدوثها عبر التاريخ ولكنها اليوم ترتكب في بيئة جديدة بوسائل حديثة وضحايا من نوع جديد. وتشكل «جرائم قطاع الأعمال» (Business Crimes) قطاعًا كبيرًا من هذه الجرائم. هناك أيضًا نوع من جرائم نظم المعلومات يمكن أن نطلق عليها «جرائم بلا ضحية» مثل البغاء وتهريب المخدرات والانتحار، أو جرائم ترتكب ضد الأشخاص مثل الخطف وانتهاك الخصوصية الفردية.

ونحاول في الجدول التالي (٣ ـ ١) أن نصنف بعض جرائم نظم المعلومات:

جرائم عامة	جرائم مادية	جرائم اقتصادية	جرائم ضد الأفراد
أخطاء الأداء المتعمدة.	السرقة.	النصب والاحتيال.	القذف والتشهير.
إغفال الواجب.	التدمير والإتلاف.	الاختلاس.	تسهيل الدعارة.
التجاهل.	تمزيق المستندات.	التلاعب.	انتهاك الخصوصية
التهور والطيش.	التعدي على الممتلكات.	الرشوة.	الإهانة.
التقصير والإهمال.	السطو الليلي.	الابتزاز.	التحرش الجنسي.
التآمر والتواطؤ.	التهريب.	التهديد.	الخطف.
	انتحال الشخصية.	انتهاك الأسرار الاقتصادية.	القتل.
	قرصنة البرامج.	التزييف والتزوير.	الانتحار.
	التجسس العسكري.		
	التجسس الصناعي.		
	التجسس الاقتصادي		

جدول رقم (٣ ـ ١) تصنيف جرائم نظم المعلومات

٣ . ٢ تخريب المعلومات وإساءة استخدامها

تتضمن جرائم نظم المعلومات جريمة «تخريب المعلومات» (abuse) ويقصد بذلك الأذى الذي يقع على المعلومات، مثل إتلافها أو تحويرها أو جعلها غير ذات فائدة (كتشفيرها باستخدام مفتاح مجهول مثلاً) . كما تتضمن جرائم نظم المعلومات كذلك جريمة «إساءة استخدام المعلومات» (misuse) والمقصود بها الأذى الذي يتم تحقيقه باستخدام هذه المعلومات مثل عدم تمكين المستفيد من الوصول إليها أو كشفها أو استغلالها في إلحاق الضرر بمصالح صاحب المعلومات . إلى جانب الضرر المباشر الذي تسببه هاتان الجريمتان، فهناك أيضًا الضرر غير المباشر الذي يلحق بالأشخاص أو الممتلكات أو حتى الخدمات التي تقدمها المؤسسات التي تقتني هذه المعلومات التي وقعت عليها الجريمة . ومهمة أمن المعلومات هنا هي منع الأضرار المباشرة وغير المباشرة معًا، فنحن لا نعرف مسبقًا بالضبط ماذا سيكون هدف المجرم، فالحل هو الحماية ضد كل أنواع الضرر التي يمكن أن تلحق بالمعلومات .

تعتبر جريمة تخريب المعلومات من جرائم نظم المعلومات الخطيرة، وتكمن خطورتها في آثارها بالغة السوء على الجهات التي تتعرض لها . والتخريب يمكن أن يتم بمحو الملفات أو تدمير الوسائط التي تحتويها . ونود هنا أن نشير إلى وسيلة خطيرة لتخريب المعلومات وهي أن يقوم المجرم بتشفير هذه المعلومات والاحتفاظ بمفتاح الشفرة وعدم الكشف عنه . وتزداد فرصة حدوث هذه الجريمة كلما قل الانضباط بين الموظفين في الشركات والمؤسسات وكلما تراخت الرقابة على الموظفين الذين لديهم صلاحية التشفير، ويمكن أن تؤدي هذه الجريمة إلى أضرار هائلة للشركة .

والمعلوم أن تشفير المعلومات هو أفضل وأقوى أساليب أمن المعلومات على الإطلاق، ولكن للأسف ففي مقدور أي شخص أن يسيئ استخدام هذه الوسيلة الأمنية فهناك الكثير من البرامج وأجهزة التشفير المتاحة للمستفيدين العاديين لتمكنهم من تشفير البيانات الخاصة بهم بحيث لا يستطيع غيرهم فك هذه الشفرة، فإذا فشلت عملية فك الشفرة (وهذا يحدث أحيانًا) لسبب ما أو إذا نسي المستفيد مفتاح الشفرة أو تعمد عدم الإفضاء به فإن المعلومات المشفرة يمكن اعتبارها في حكم المفقودة نهائيًا ولا سبيل إلى استعادتها مرة أخرى. وبعض المعلومات التي يُراد الاحتفاظ بها لمدد طويلة مثل ملفات تسجيل المعاملات (Logs) معرضة لخطر الفقد إذا تقادمت برامج التشفير التي استخدمت في تشفيرها أوتم تحديثها بنسخ أحدث أو تغييرها ببرامج أخرى، ويزداد الطين بلة إذاتم (زيادة في الحرص) إعدام النسخ الأصلية (غير المشفرة) من هذه الملفات.

وتعتبر قدرة الموظف على تشفير المعلومات ثغرة أمنية خطيرة حيث قد يقوم الموظف بتشفير بعض الأسرار التجارية ونقلها (مشفرة) إلى الشركات المنافسة، وهو بذلك يستطيع أن يفلت من العقوبة حيث لا يمكن إثبات أي جرم ضده إذ أن دليل الجريمة لا يستطيع قراءته سواه.

٣ . ٣ الإهمال

قد تحدث حوادث نظم المعلومات عمدًا بفعل فاعل، أو قد يكون السبب فيها مجرد الإهمال. ومن الحوادث الشهيرة التي تعكس الإهمال هي تلك الخاصة بنظام العلاج الإشعاعي «ثيراك ٢٥» (Therac-25) وهو نظام للعلاج الإشعاعي يَستخدم معالجاً إلكترونيًا يعمل بواسطة الحاسب الآلي، وقد تسبب في ستة حوادث في الفترة من يونيو ١٩٨٥ وحتى يناير

١٩٨٧ ، ونتج عن هذه الحوادث ثلاث وفيات تم تشخيص سبب الوفاة فيها بأنه نتيجة جرعة إشعاع زائدة.

تسبب مصممو الجهاز وصانعوه في وجود ثلاث ثغرات في النظام: الأولى هي إتاحة الفرصة لمشغل الجهاز لكي يدخل التعديلات في سطر الأوامر بالحاسب المتحكم في الجهاز لتغيير وضع الآلة، وكانت النتيجة أن الآلة كانت تبدأ في تسريب الإشعاع قبل أن تبدأ التغييرات التي أدخلها المشغل في إحداث أثرها. الثغرة الثانية تمثلت في إمكان تجاوز اختبارات الأمان التي يلزم إجراؤها عندما يصل أحد عدادات البرنامج إلى الصفر. أما الثغرة الثالثة فكانت إلغاء بعض أجهزة الأمان المادية (hardware) والتي تقوم بإغلاق الجهاز آليًا عند تجاوز الإشعاع حد الأمان واستبدلوا بها برامج يسهل تعديلها، وهذه الثغرة الثالثة بالذات كانت شديدة الخطورة حيث كانت تسمح بتسرب جرعات عالية من أشعة «إكس» مباشرة إلى جسم المريض وفي أماكن عشوائية لا يجب تسليط الإشعاع عليها، وكان المفروض أن يبث الجهاز الجرعة العالية فقط عندما يكون الهدف (الورم المطلوب تسليط الإشعاع عليه) في مواجهة الجهاز لإنتاج شعاع إلكتروني يصل بأمان إلى المريض.

أظهرت هذه الحادثة كيف يمكن أن تؤدي ثغرات النظم التي تنشأ في مرحلة التصميم بشكل مباشر إلى ثغرات خطيرة عند تشغيل النظام. فمطورو النظام لم يستوعبوا بشكل جيد الطرق المختلفة التي سوف يُستخدم بها النظام وكيف سيتعامل معه المشغلون وكيف سيتعرض له المرضى، ومن ثم لم يقوموا بتقييد مستخدمي الجهاز بإجراءات أمن تضمن سلامة التشغيل. في هذه الحادثة نستطيع القول أنه لم تكن هناك شبهة تعمد ولكن من الممكن أن يقوم مجرم ما باستغلال هذه الثغرات لتعمد إيذاء المرضى أو ربما قتلهم.

٣ . ٤ إغفال الواجب

إن إغفال الواجب من جانب المسئول عن أداء مهمة تقنية يعتبر جريمة، وقد تصل نتائج هذه الجريمة إلى حد تعريض حياة الآخرين للخطر. وكمثال على ذلك نجد أن غالبية الأجهزة التي تدخل في تشغيلها دوائر إلكترونية تصدر عنها مجالات كهربية ومغناطيسية ذات ترددات متفاوتة تصل في بعض الحالات إلي ما يزيد علي ٩٠ ميجا هيرتز، مثل أجهزة التليفزيون والفيديو والهاتف اللاسلكي والهاتف الجوال وأجهزة الكمبيوتر وأجهزة الألعاب الإلكترونية وأجهزة الليزر وذلك بالإضافة إلي الأجهزة الكهربائية المستخدمة داخل المنازل مثل أفران الميكروويف وافتقارها إلي التوصيلات الأرضية الفعالة (earthing) وما يترتب على ما يصدر منها من مجالات مغناطيسية تتراوح شدتها بين ٥ حتي ٨ جاوس وترددات موجاتها بين ٥ حتى ٥٠ هيرتز. وتصاحب هذه المجالات مجالات كهربية لها الترددات نفسها وتتراوح شدتها على سطح هذه الأجهزة ما بين ٢٠ حتى ٣٠ كيلوفولت على المتر المربع خاصة إذا ما أخذنا في الاعتبار المنازل والمدارس والمستشفيات ومواقع العمل القريبة من أبراج البث الإذاعي والتليفزيوني واللاسلكي ومحطات اتصالات الأقمار الفضائية ومحطات الرادار ومحطات تقوية إرسال واستقبال الهاتف الجوال، بالإضافة إلى كابلات خطوط الجهد العالي. فعلى سبيل المثال يصل المجال الكهربي على سطح جهاز تليفزيون من قياس ٢٢ بوصة إلى ٣٠ كيلوفولت على المتر المربع وبترددات تصل إلى ١٢ كيلوهيرتز. هذا ومن الملاحظ تزايد معدلات استخدام أجهزة توليد الموجات المغناطيسية التي تتراوح شدتها من ٢٠٠ حتى ١٦ ألف جاوس (Alqady,1999).

ويتعرض جسم الإنسان لامتصاص الطاقة الإشعاعية من مصادرها الطبيعية والصناعية تعرضًا خارجيًا وداخليًا بفعل النشاط الإشعاعي للبيئة المحيطة والمواد المشعة الممتصة داخل الجسم، وتزداد احتمالات حدوث الأمراض الإشعاعية مع زيادة مستوى الجرعة الإشعاعية الممتصة داخل أعضاء الجسم المختلفة من ثم وضعت الضوابط التي تكفل عدم السماح بأي تعرض إشعاعي يترتب عليه أضرار قطعية بأنسجة وخلايا الجسم الحية وقصر التعرض الآمن على أدنى مستوى يمكن الوصول إليه لتحقيق الهدف الطبي أو المهني أو التكنولوجي من هذا التعرض. إلا أن تحديد المستويات الآمنة للتعرض الإشعاعي لا تضمن عدم استحداث الأضرار الاحتمالية التي قد تنشأ بعد فترات زمنية طويلة سواء في الأفراد الذين تعرضوا لهذه المستويات أو أجيالهم المقبلة. وإذا كان من اللازم أن تصل الجرعات الإشعاعية الممتصة إلى مستوى محدد حتى يمكنها أن تحدث الأضرار القطعية الحادة إلا أن بلوغ هذا المستوى ليس ضروريًا لاستحداث الأضرار الاحتمالية التي منها الأورام السرطانية والأمراض الوراثية، حيث إنه يمكن لأصغر الجرعات الإشعاعية إحداث الأضرار البيولوجية المتأخرة. إلا أنه يجدر الأخذ في الاعتبار أنه ليس هناك تجانس بين الأفراد في هذه الاستجابة البيولوجية للتعرض الإشعاعي إذ قد يتأثر بها فرد دون الآخر، أو عضو حي دون العضو الآخر. ويرجع ذلك إلى العديد من الأسباب البيولوجية والبيئية ومنها اختلاف معدلات ميكانيكية الجسم الحي في إصلاح الأضرار التي تلحق بالأنسجة والخلايا الحية وعمر الإنسان ومستوى تعرض الفرد لعوامل بيئية مؤثرة تلحق الضرر بالمادة الوراثية الخلوية ومن هذه العوامل الملوثات الكيميائية والميكروبات ودرجات الحرارة العالية. وقياسًا على ذلك، فإن تعرض شخص ما لجرعة إشعاعية لا يعني على وجه اليقين أن

قدره يحتم إصابته بالأورام السرطانية أو تعرض ذريته للأضرار الوراثية إلا أنه يكون في الغالب معرضا بدرجة أكبر لمواجهة مثل تلك الأضرار إذا ما قورن بحالته إذا لم يكن قد تعرض لمثل تلك الجريمة الإشعاعية ويزداد احتمالات مثل تلك الأضرار مع تصاعد مستوى الجرعة التي تعرض لها .

ولقد شهد العقد الحالي تصاعدا مطردا للبحوث التي تجرى حول الأضرار البيولوجية للتعرض للمجالات الكهربية والمغناطيسية والإشعاعية بمستوياتها العالية والمنخفضة وتجري الدراسات على حيوانات التجارب، بالإضافة إلى عمل إحصائيات عن أنواع الأمراض الشائعة بين المتعرضين لهذه المجالات وقد سجلت النتائج عديدًا من هذه الأمراض منها زيادة حساسية الصدر والجلد والعين والصداع المزمن والتهاب المفاصل وهشاشة العظام والتوتر والرعب والانفعالات غير السوية وأعراض الشيخوخة المبكرة والإحباط وتليف عضلات القلب والعجز الجنسي والاختلالات الوظيفية للمخ والأعصاب وأمراض الدم وعتامة عدسة العين البللورية والتشوهات الخلقية .

ومن ثم فالأمر يتطلب النظر في كيفية رصد مصادر التعرض للمؤثرات المختلفة وأخذ معدلات هذا التعرض في الاعتبار عند تحديد الجرعة الآمنة للتعرض الإشعاعي خاصة للسيدات في مراحل الحمل المبكرة~ . ~ كما يجدر الاهتمام برفع مستوي الوعي الجماهيري بالتأثيرات الضارة للتعرض للمجالات الكهربية والمغناطيسية والإشعاعية والضوابط الأخلاقية التي تنظم القابة على تداول مصادرها (Alqady,1999) .

٣ . ٥ تزوير البيانات

ربما كانت جريمة «تزوير بيانات الحاسب» هي أكثر جرائم نظم المعلومات انتشارًا على الإطلاق، فلا تكاد تخلو جريمة من جرائم نظم المعلومات من عملية تزوير للبيانات بشكل أو بآخر. ويتم تزوير بيانات الحاسب إما بإدخال بيانات مغلوطة إلى قواعد البيانات أو بتعديل البيانات الموجودة عمدًا بهدف ارتكاب جريمة من جرائم نظم المعلومات. وهذا العمل لا يتطلب بالضرورة معرفة بالبرمجة ولكن يتطلب معرفة بسيطة بكيفية استخدام التطبيق كتطبيقات المرتبات أو تطبيقات الحسابات في البنوك وغيرها، وللأسف فإن الموظفين المسموح لهم بإدخال البيانات ثبت أنه كان لهم ضلع كبير في الكثير من جرائم نظم المعلومات مثل تغيير أرصدة الحسابات وتزوير المعاملات والتخريب وسرقة المخزون وتزوير المرتبات.

وكمثال على هذا النوع من الجرائم هناك قصة مدخلة البيانات التي كانت صديقة لرئيس نادي السيارات في مدينة «سكرامنتو» بولاية كاليفورنيا بالولايات المتحدة. فقد قامت هذه الفتاة بتغيير ملكية السيارات المسجلة في الحاسب بحيث تصبح مسجلة باسم بعض لصوص السيارات، ثم يقوم هؤلاء اللصوص بسرقة هذه السيارات. وكان الضحايا من أصحاب السيارات المسروقة يفاجأون عند تقدمهم للشرطة للإبلاغ بسرقة سياراتهم بأنه لا يوجد في سجلات الحاسب ما يثبت ملكيتهم لهذه السيارات التي يبلغون بسرقتها. وبعد أن يقوم اللص بالتصرف في السيارة بالبيع على أنها مملوكة له (فالسيارة مسجلة باسمه في سجلات الحاسب) تقوم هذه الفتاة بإعادة السجلات لسابق عهدها حيث تعود لتظهر ملكية صاحب السيارة الأصلي لها. وكانت مدخلة البيانات تقدم هذه الخدمة في مقابل مائة دولار

للعملية الواحدة حتى تم القبض عليها بعد أن اعترف عليها أحد اللصوص، ومن ثم قام أحد رجال الشرطة السريين بالتعامل معها على أنه أحد لصوص السيارات ودفع لها المبلغ المعلوم ووقعت في يد العدالة.

من الوسائل المتبعة لتزوير بيانات الحاسب وسيلة تعديل البيانات باستخدام بعض البرامج المساعدة الجاهزة (Utilities) المصممة خصيصًا لتعديل البيانات في أماكنها مباشرة (Superzapping). وهذا النوع من البرامج خطير لأنه لا يترك أثرًا يدل على التعديل أو القائم بالتعديل، ولذلك يجب تحديد الأشخاص المسموح لهم باستخدام هذه البرامج وأن يتم ذلك في أضيق نطاق. ونحن لا نستطيع أن نمنع هذا النوع من التعديلات تمامًا لأنها وسيلة مفيدة في أحوال كثيرة ولا يمكن إلغاؤها، وإنما على خبراء أمن المعلومات ألا يغفلوا عن هذه الثغرة.

وكمثال على هذا النوع من الجرائم تلك الحادثة التي قام فيها مشرف تشغيل الحاسب في أحد البنوك في «نيوجيرسي» باستخدام برنامج مساعد لزيادة أرصدة حسابات العديد من الأصدقاء، ثم يقوم هؤلاء الأصدقاء بسحب هذه الأموال، وبعد ذلك يعمد هذا المجرم إلى تمزيق إيصالات السحب. وكان في تخطيطه أن يوقف هذه السرقات قبل موعد المراجعة الدورية لحسابات البنك تفاديًا لكشف جريمته، ولكن (أصدقاءه) كانوا أشد طمعًا مما جعلهم يرفضون التوقف ويجبرونه على الاستمرار. وعند حلول موعد المراجعة الدورية اكتشف المراجعون هذه العمليات لأنها كان قد تم تسجيلها بواسطة نظام أمن سري كان يقوم بتسجيل كل العمليات على الحاسب الموجود في أحد الفروع البعيدة للبنك، وكان المجرم لا يعرف شيئًا عن هذا النظام الأمني. وقام المراجعون بتحقيق طويل ومراقبة مضنية لمعرفة

من لديه الصلاحية والمعرفة لتنفيذ هذه التعديلات، ومن سوء حظ مشرف التشغيل هذا أنه كان الوحيد الذي أشارت إليه أصابع الاتهام.

٣ . ٦ التزييف

يقوم الآن بعض مجرمي نظم المعلومات بتزييف الوثائق وصنع وثائق مقلدة وذلك بتكلفة بسيطة للغاية وبدرجة معقولة جدًا من الدقة التي تخدع الكثيرين. ومن بين الوثائق الورقية التي يجرى تزييفها الشيكات المصرفية وتذاكر المباريات وتذاكر السفر (في عام ١٩٩٢) تمت إدانة المقتحم «كابنكرنش» ومجموعة من زملائه بتهمة تزييف تذاكر السفر لعبارة خليج «سان فرانسيسكو»)، وحتى الأسهم والسندات أيضًا يتم تزييفها. ولا يحتاج المزور إلى أكثر من حاسب شخصي رخيص الثمن به برنامج للرسوم (Graphics)، وإلى جهاز ماسح ضوئي (Scanner) لمسح الوثائق وتحويلها إلى نصوص رقمية، وإلى الأنواع المناسبة من الورق التي تشابه الورق المستخدم في الوثائق الأصلية، بالإضافة إلى طابعة ملونة عالية الكفاءة. وفي أوساط طلبة الجامعات في أوروبا والولايات المتحدة تنتشر عمليات تزييف تذاكر المباريات الرياضية والحفلات، وأخشى أن أقول أن الشهادات الدراسية أيضًا أصبحت الآن هدفًا للتزييف في مناطق كثيرة من العالم. وفي بعض الدول العربية يتم استخدام الحاسب الآلي والطابعات الملونة في تزييف العملة مما دعا الكثير من الدول إلى إضافة المزيد من إجراءات الأمن في أوراقها المالية كالأشرطة المعدنية والعلامات المائية واستخدام أنواع الورق النادرة وغير ذلك من الإجراءات.

وقد يلجأ المزيف إلى سرقة الأجهزة الضرورية لمساعدته في التزييف إذا عجز عن شرائها من الأسواق، ففي عام ١٩٩٦ اشترت حكومة ولاية

«فلوريدا» أجهزة حاسب خاصة لإصدار رخص القيادة، وتضمنت هذه الأجهزة كل الضمانات التي تجعل من شبه المستحيل تزييف رخص القيادة، ولما كانت هذه الأجهزة والأدوات غير متاحة في الأسواق فقد قام اللصوص باقتحام مكتب إصدار رخص القيادة وسرقة أجهزة الكمبيوتر والأوراق والأدوات المستخدمة في عملية إصدار الرخص، وتكررت هذه العملية في خمسة مكاتب!!.

وتنجح الشرطة عادة في تقديم مرتكبي جرائم التزييف بواسطة الحاسب الآلي للمحاكمة، كما تنجح في تقديم أدلة الإدانة بسبب خبرتها في جرائم التزييف بصفة عامة بغض النظر عن الوسيلة التي يتم بها التزييف.

في عام ١٩٨٨ أدين مجرم كندي باستخدام آلة ملونة لتصوير المستندات لطبع ٢٤ ألف دولار مزيفة من فئة الخمسين دولارًا والمائة دولار. وقد قامت إحدى العصابات بتزوير شيكات مصرفية مزيفة منسوبة لأحد البنوك في ولاية «مين»، ولكن العصابة وقعت في خطأ فادح عندما استخدمت في طباعة هذه الشيكات رموز الحبر المقروء (MICR) الخاصة ببنك آخر في ولاية «فلوريدا». وتم تبادل هذه الشيكات بين البنكين عدة مرات، فكان البنك الأول يعيدها للبنك الثاني بعد فرها بالكمبيوتر (بناء على رموز الحبر المقروء)، والبنك الثاني يعيدها للأول بمجرد نظر الموظفين للشيك (لأن الشيك مطبوع على أوراقه) حتى تم اكتشاف الجريمة عندما لاحظ موظف التحويلات في أحد البنكين أن اسم فرع البنك المطبوع على الشيك كان به خطأ هجائي. ولكن ذلك جاء متأخرًا بعد فرار المجرمين بمبلغ لا بأس به.

يمكن مكافحة هذا النوع من الجرائم باستخدام نظام «تبادل الوثائق الإلكتروني» (EDI) أو (Electronic Data Interchange) وهو الأسلوب

المستخدم في أجهزة الإيداع الآلي في البنوك وأسلوب السفر بدون تذاكر وهو أيضًا نفس أسلوب «النقود الإلكترونية» الذي نتعرض له في هذا الكتاب بالتفصيل. هذه الخدمات الآلية تتلافى استخدام الوثائق الورقية التي يمكن تزييفها بسهولة. ولكن لأن استخدام الأوراق متغلغل في ثقافتنا إلى حد بعيد فإن كثيرًا من الشركات تلجأ في مكافحة هذا النوع من الجرائم إلى استخدام أنواع معينة من الأحبار في وثائقها أو بعض الأشرطة المعدنية أو العلامات المائية في الأوراق التي تطبع عليها وثائقها أو شهاداتها أو أسهمها، وربما تلجأ إلى أسلوب «الطباعة الغائرة» أو «شعار الخلفية» على الوثائق، أو يلجأون إلى طباعة الأحرف الدقيقة التي لا تُرى إلا بالمجهر على أجزاء من الورقة. كما تقوم الشركات، ويجب أن تفعل ذلك، بتدريب موظفيها على الاهتمام بكشف أي احتمالات تزييف للوثائق.

٣ . ٧ الابتزاز

عمليات الابتزاز هي من جرائم نظم المعلومات، وهي قد ترتكب من جانب موظفي المؤسسة الحاليين أو السابقين أو المؤقتين، كما قد ترتكب من جانب الموردين أو العملاء كذلك. وهناك أكثر من حالة قام فيها مطور نظام المعلومات بزرع قنبلة منطقية في النظام الذي تعاقد على تصميمه، وقد صممت القنبلة بحيث تدمر البيانات أو توقف عمل النظام إذا لم تقم الشركة بدفع كامل مستحقات المبرمج.

تشجع حالات عدم الرضا الوظيفي بعض الموظفين على ارتكاب هذا النوع من الجرائم خاصة عند قيام الشركة بفصل بعضهم خلال إجراءات تخفيض العمالة مثلاً.

لتلافي ارتكاب هذا النوع من الجرائم ننصح بفصل النظم التجريبية عن النظم الإنتاجية بحيث لا يستطيع المبرمج أن يتعامل مع التطبيق بعد إجازته ونقله إلى البيئة الإنتاجية، كما ينصح بمرور جميع البرامج باختبار الجودة للتأكد من خلوها من أي ثغرات أو قنابل منطقية مثلاً.

٣ . ٨ تزوير العلامات التجارية

تشكو بعض الشركات المنتجة لشرائح المعالجات المركزية مثل شركة «إنتل» من ظاهرة خطيرة تضر بمصالح هذه الشركات كما تضر بمصلحة المستفيد، وهي تزوير العلامات التجارية على الشرائح ذات الأداء المنخفض، وبيعها على أنها شرائح ذات أداء أعلى بأسعار أكثر ارتفاعًا. ويلجأ بعض موزعو هذه الشرائح وبعض منتجو أجهزة الحاسب الشخصي إلى ارتكاب هذه الجريمة سعيًا وراء المزيد من الربح وبحثًا عن التفوق في المنافسة. وفضلاً عما يسببه ذلك من أضرار مؤكدة للمستفيد وللشركات المنتجة التي يتم تزوير علاماتها، فإن ذلك يفقد المستفيدين الثقة فيما يحصلون عليه من الأسواق.

٣ . ٩ انتهاك الخصوصية

الخصوصية الفردية هي حق الإنسان في حجب معلوماته الشخصية عن الآخرين. ويعتبر التطفل على مكتب شخص آخر أو منزله أو جهاز الحاسب الشخصي الخاص به، أو حتى أفكاره يعتبر انتهاكًا لهذه الخصوصية. وبالتطفل لا نعني تدمير المعلومات أو تحويرها، بل إن مجرد فتح الحاسب الشخصي الخاص بشخص ما والاطلاع فقط على ما به من بيانات هو انتهاك للخصوصية الفردية للإنسان.

فهل أدى انتشار استخدام الحاسب الشخصي إلى زيادة تعرض الخصوصية الفردية للإنسان لخطر الانتهاك؟ أم أنه قلل من ذلك؟ هذه قضية يثور حولها الجدل، فبعض الناس يرون أن إخراج بياناتك من الأدراج والملفات (أو من رأسك) وجمعها كلها في مكان واحد هو الكمبيوتر يزيد من خطر تعرضها للانتهاك. ويرون كذلك أن عدم تعود الناس على أساليب تأمين المعلومات وعدم إلمامهم بهذا الفن يزيد أيضًا من خطر تعرض معلوماتهم للانتهاك، كما يلمحون إلى الانتشار الحالي الذي يحظى به استخدام شبكات المعلومات، مما يعني أن معلوماتك الآن (تسري) في الهواء بعد أن كانت حبيسة غرفتك أو خزانتك.

وعلى الجانب الآخر يرى فريق آخر (وأنا منهم) أن وجود المعلومات في حيز ضيق محدود (في الحاسب) واتباع الأساليب الصحيحة لتأمين البيانات من تشفير (تعمية) وكلمات مرور وغيرها يجعل معلوماتك أكثر أمنًا مما كانت عليه في ملفاتك أو أدراج مكتبك حيث يمكن أن يطلع عليها خلسة السكرتير أو عامل النظافة، كما أنه لا خطر في حالة الحاسب من أن تنسى مفاتيحك مرة فيتم نسخها، بل مع الحاسب تستطيع تغيير كلمة المرور كلما شئت ذلك، بل إن بعض نظم أمن المعلومات تفرض استخدام كلمة مرور جديدة في كل مرة تدخل فيها إلى الحاسب.

ولكن ماذا عن معلوماتك الشخصية الموجودة على الإنترنت؟ فأنت عند اتصالك بأي موقع على الإنترنت فإما أن يترك هذا الموقع على جهازك بعض الملفات الصغيرة (Cookies) أو يحصل منك، سواء برغبتك أو دون أن تدري على الكثير من المعلومات المسجلة في حاسبك الشخصي. وتقوم بعض المواقع المشبوهة بنسخ بعض الملفات التي يظن أنها قد تكون ذات

فائدة له مثل الوثائق المخزنة على الحاسب، والإنسان يكون في العادة أقل ترددًا عندما يفشي معلوماته الشخصية للكمبيوتر وليس لإنسان آخر.

وماذا عن معلوماتك الموجودة لدى العديد من الجهات الرسمية؟ سواء معلوماتك الصحية أو المهنية أو التعليمية أو غير ذلك. كيف تضمن الاحتفاظ بسريتها؟ خاصة عندما تبدأ كل هذه الجهات في (ميكنة) معلوماتك وحفظها على الحاسب مما يسهل فرزها وتصنيفها والوصول إلى المطلوب منها بسهولة ويسر.

لتأمين المعلومات الشخصية للأفراد يجب استخدام أكثر من وسيلة، فمثلاً نلجأ إلى تشفير هذه المعلومات وتسمية الأشخاص المسموح لهم بالاطلاع عليها أو تعديلها أو استخدامها بحيث يكون في أضيق نطاق ممكن. كما يجب تجهيز نسخة احتياطية من هذه المعلومات تفاديًا لفقدها، والاحتفاظ بسجل عمليات يبين كيف ومتى وبواسطة من تم التعامل مع هذه البيانات.

وفي بعض الشركات يُسمح للموظفين أنفسهم بتحديث بياناتهم الشخصية من خلال الحاسب الشخصي، ويتم ذلك دون أن يتعرضوا للحرج من الإفضاء ببيانات معينة لموظفي إدارة شئون الموظفين.

٣ . ٩ . ١ حماية الخصوصية الفردية

تبدأ حماية الخصوصية الفردية للأشخاص بالاهتمام بدقة المعلومة وتكاملها وأمنها وما يحدث لها حتى يتم حفظها دقيقة وأن يجري تأمينها ضد الاستخدام غير المصرح به.

وتتوافر الخصوصية حينما نستطيع التفرقة بين المعلومات التي لها طابع الشخصية وتلك التي يمكن كشف النقاب عنها، مع تحديد في أي وقت

وبأي كيفية يتم هذا الكشف. ولكي نضع سياسات مناسبة لحماية خصوصياتنا يجب معرفة السبل المختلفة التي يأتينا منها الخطر.

٣ . ٩ . ٢ كيف يمكن وقف تسرب المعلومات الشخصية؟

من الصعب جدًا السيطرة على ما يحدث للمعلومة بمجرد خروجها من جهاز الحاسب، وعلى ذلك فإن حماية الخصوصية يجب أن تبدأ من البداية بتحديد نوعية البيانات التي لا ينبغي أن تصبح عامة ومشاعة ثم بتقييد الوصول إلى هذه البيانات.

ولكن هناك عدد من العوامل الأساسية تجب مراعاتها عند تحديد نطاق الخصوصية الفردية لأفراد المجتمع، منها أنه ينبغي تحديد البيانات الشخصية من جانب الهيئات العامة أو الخاصة بحيث يمكن تزويد هذه الجهات ومثيلاتها بالمعلومة المطلوبة ثم إعدام هذه المعلومة عندما لا تصبح هناك حاجة إليها.

كما يجب أن يقتصر استخدام المعلومات فقط على الغرض الذي وافق عليه صاحب المعلومات وألا يسمح بتداولها إلا من خلال موافقة كتابية صريحة من صاحب المعلومة أو ممن كانت المعلومة تضر بمصالحه المشروعة، وكذلك ضمان حماية أمن وسائل الاتصال الإلكتروني لتحقيق الهدف الأصلي وهو السماح للمعلومة بالانتقال من المرسل إلى المستقبل دون تبديلها أو اعتراضها في الطريق أو الكشف عن محتواها~ لأي طرف آخر.

كما ينبغي فرض السياسات التي تضمن تداول المعلومة بالطرق التي تحمي سلامتها وتكاملها~ على جميع الجهات فبرغم أنه قد سبق وأن أثارت المنظمة العالمية للتعاون الاقتصادي والتنمية وكذلك الاتحاد الأوروبي مثل هذه المبادئ إلا أن هناك شكاً في أن تلتزم شركات المعلومات أو الشركات الخاصة بالأخذ بهذه السياسات من تلقاء نفسها.

كما يلزم إحاطة المتفعين بالمعلومة بما تنطوي عليه الخصوصية بالنسبة لوسائل الاتصال القائمة أو المستحدثة وما قد يستجد من تقنيات تتعلق بها .

ويجب إعداد الآليات الفعالة التي تكفل مراعاة تنفيذ هذه المبادئ التي تحمي الفرد والهيئات والشركات وغيرها دون انتظار لتدخل الحكومات .

٣ . ٩ . ٣ هل التنصت الحكومي مباح؟

هناك تضارب بين حق الفرد في الحفاظ على خصوصيته الفردية وحاجة الدولة لاختراق هذه الخصوصية لفرض القانون ومنع الجريمة . هذا التضارب بدأ عالميًا في عام ١٩٨٢ عندما لجأت بعض الدول إلى التنصت الهاتفي لمحاربة الجريمة (Bowyer,1996) . وبتطور الحاسب الآلي وانتشار استخدام المعلومات زاد هذا التضارب بين الحاجة إلى اختراق الاتصالات وحق الخصوصية الفردية .

ونلاحظ أن تقنية الحاسب آخذة في التعقيد بشكل يخشى معه أن يهدد قدرة المسئولين عن حماية القانون على ممارسة تنصت يسهل مهمتهم .

ويدور جدل كبير حول جدوى ومشروعية اختراق الاتصالات في الحرب ضد الجريمة . فتقول «سوزان لاندو» (ترى الجهات الأمنية أن اختراق الاتصالات ضرورة حتمية ليس فقط لأن ذلك يتيح الحصول على معلومات لا يمكن الحصول عليها بوسائل أخرى ، ولكنه أيضًا يقدم الأدلة التي تكون لها قيمة ملموسة ويعتمد عليها إلى حد كبير ، ووفقًا لمصادر مكتب التحقيقات الفيدرالي FBI فإن الجريمة المنظمة تراجعت بشكل كبير نتيجة استخدام وسائل اختراق الاتصالات) (Landau et al 1994 b) كما أن اختراق هذه الاتصالات يساعد كثيرًا في الحصول على اعترافات المتهمين . وتكتسب هذه الوسيلة أهمية خاصة في صراع أجهزة الأمن مع

عصابات تجارة المخدرات وتعتبر تقنية تحقيق هامة في حالات الفساد الحكومي والعمليات الإرهابية .

ولكن «جون بارلو» يقول (حتى لو كانت هذه التهديدات حقيقية فهل اختراق الاتصالات هو أفضل الوسائل لمواجهة هذه التهديدات؟ من الواضح أن ذلك لم يكن صحيحًا في الماضي ، وعبر السنوات العشر الماضية كان متوسط عدد التصاريح التي منحت لاختراق الاتصالات على مستوى الولايات المتحدة أقل من ٨٠٠ تصريح في العام ، أي إن هذه الوسيلة ، على الأقل في الوقت الحاضر ، لا توفر دليلاً حاسمًا لإدانة المجرمين ، وهي في هذا الصدد أقل فعالية بكثير من شهادة الشهود أو القرائن والأدلة المادية أو ما يقوم به المخبرون التقليديون) (Barlow,1993) .

٣ . ٩ . ٤ الخصوصية الفردية في العالم المتقدم

في أوروبا تعترف دول الاتحاد الأوروبي بحق الخصوصية كمبدأ (باستثناء بلجيكا واليونان وإيطاليا وأسبانيا التي لم نتمكن من التأكد إذا كان لديها تشريعات لحماية الخصوصية الفردية) وتقوم الدول التي تعترف بحق الخصوصية بسن التشريعات التي توفر حماية واضحة للبيانات الشخصية للأفراد ، خاصة عندما يتم تخزينها على الحاسب الآلي ، وذلك بمنع استخدامها سواء داخل الدولة العضو في الاتحاد أو إذا تم نقلها إلى دول أخرى . وهذه التشريعات تختلف من دولة لأخرى وفقًا لنوع وطبيعة المعلومات التي تحميها كما تختلف من حيث الوسائل التي تتم من خلالها هذه الحماية .

كان الدافع الرئيسي لاهتمام بعض الدول الأعضاء هو الإيمان بالخصوصية الفردية ، بينما كان دافع البعض الآخر هو الرغبة الشديدة في التناغم مع الدول الأخرى الأعضاء ، إذ كان ذلك أحد شروط الانضمام

إلى الاتحاد. لذلك نجد أن الدول الأعضاء تختلف في درجات حمايتها للخصوصية الفردية فبعضها يحمي المعلومات الشخصية المخزنة على الحاسب والخاصة بالأفراد الأحياء فقط، والبعض الآخر (الدانمارك والنمسا) يمد مظلة هذه الحماية إلى الشخصيات الاعتبارية مثل الشركات والنقابات وغيرها، بينما نرى دولاً أخرى (فرنسا وألمانيا وهولندا) تمد مظلة الحماية إلى أبعد مدى فتحمي البيانات الورقية وبيانات الحاسب وجميع أنواع البيانات الشخصية أيًا كان الوسط الذي تقع عليه (Carr,1994) .

في بعض البلاد خارج نطاق الاتحاد الأوروبي تقتصر حماية البيانات على حالة استخدامها بشكل علني (الولايات المتحدة ونيوزيلندة)، وواضح أن الهدف هنا هو حماية الفرد من التشهير فقط .

٣ . ٩ . ٥ الخصوصية الفردية في العالم الثالث

أما دول العالم الثالث (أمريكا اللاتينية وأفريقيا) فقد اقترحت أن الحماية يجب أن تشمل المعلومات التي تمس اسيادة الوطنية أو الرخاء الاقتصادي أو المصالح الثقافية والاجتماعية للشعوب. ويتضح هنا أن الحظر هو في الحقيقة لصالح الدولة أو مجموع الشعب وليس لصالح الأفراد، وهو يتخذ غطاء لحماية الحكومات. فعندما أصدرت حكومة جمهورية مصر العربية تشريعًا (نشر بجريدة الوقائع المصرية عام ١٩٨٦) يقضي بسرية بيانات الأرصدة في البنوك وعدم جواز إفشائها حتى للإدارات الحكومية، لم يطلق المشرع هذا الحكم بلا استثناء ولكنه استثنى الحالات التي يصدر بها أمر من النيابة العامة وفرض على البنوك الامتثال لمثل هذه الأوامر. بينما نرى الحكومة السويسرية والبنوك جميعها في الاتحاد السويسري تمنح حماية كاملة وسرية لا استثناء فيها على أرصدة العملاء وحساباتهم وحركة هذه الحسابات. ومن المفهوم أن الدافع وراء هذا الاتجاه هو دافع اقتصادي بحت (داود، ٢٠٠٠).

الفصل الرابع

التجسس

٤ . ١ التجسس العسكري .

٤ . ٢ التجسس الصناعي .

٤ . ٣ التجسس التجاري .

٤ . ٤ أساليب جديدة للتجسس .

٤ . ٥ أثر التواطؤ في جرائم نظم المعلومات .

التجسس

نتطرق في هذا الفصل إلى جريمة نمت وازدهرت في عصر المعلومات، واتخذت أبعادًا جديدة وآفاقًا أرحب مع تطور الحاسبات والشبكات ووسائل الاتصال. هذه الجريمة هي جريمة التجسس بأنواعه المختلفة، ونتعرض في هذا الفصل لنبذة عن تاريخ التجسس الإلكتروني وكيف بدأ، ثم نتحدث عن التجسس العسكري والتجسس الصناعي ونضرب له أمثالاً ونبين كيف أن التجسس وجريمة نظم المعلومات بشكل عام يكون ارتكابها أكثر سهولة في الشركات الصغيرة. نتحدث في هذا الفصل أيضًا عن التجسس التجاري الدولي ونذكر بعض الأساليب الجديدة التي تجعل «التجسس الآلي» ممكنًا، ثم نختتم الفصل بالحديث عن أثر التواطؤ في جرائم نظم المعلومات لأن شبكات التجسس تحتاج كثيرًا إلى «شخص من الداخل».

٤ . ١ التجسس العسكري

قبل انهيار الاتحاد السوفيتي السابق كان هناك أقل من ٣٠ خط هاتف دولي مسموح بها بين موسكو والعالم الخارجي بأكمله (Hutt,1995)، وبرغم أن ذلك لم يُعلن صراحة، إلا أنه من السهل استنتاج أن سبب هذا التحديد المبالغ فيه لعدد الخطوط هو تسهيل الرقابة والتنصت على المكالمات الدولية بين الاتحاد السوفيتي والعالم، فمراقبة عدد محدود من الخطوط أمر سهل وممكن بينما مراقبة عشرة آلاف محادثة هاتفية تتم في نفس الوقت يكون مكلفًا للغاية لو تم يدويًا. أما التنصت على خطوط البيانات فهو أمر آخر صاحبته تطورات عديدة عبر سنوات هذا القرن.

نستطيع القول بأن عصر التجسس الإلكتروني بدأ في الرابع من أغسطس من عام ١٩١٤، ففي ذلك اليوم تعمدت سفينة الكابلات البريطانية

«تلكونيا» قطع الكابلات البحرية الخمسة التي تربط ألمانيا بالعالم الخارجي والتي كانت ترقد على عمق كبير في مياه البحر المتوسط، ونتيجة لذلك اضطرت الحكومة الألمانية للتحول إلى استخدام وسيلتين إستراتيجيتين للاتصال: الأولى كانت البرقيات اللاسلكية، والثانية كانت الرسائل المشفرة التي كانت ألمانيا تقوم بإرسالها عبر طرف ثالث يكون على اتصال بباقي الكابلات البحرية الأخرى التي كانت المملكة المتحدة تملكها وتقوم بتشغيلها. وعلى الفور قامت البحرية البريطانية بمحاولات التقاط وفك شفرة هذه الرسائل، الأمر الذي أدى فيما بعد إلى التقاط وفك شفرة برقية «زيمرمان» الشهيرة مما نتج عنه دخول الولايات المتحدة الحرب العالمية الأولى.

في الأيام الأولى لهذه الحرب (الأولى) وبسبب التقدم السريع لجيش الإمبراطورية الألمانية في فرنسا فقد ظهر لدى الألمان نقص شديد في الكابلات المستخدمة في خطوط البرق، وهو الأمر الذي لم يولوه أهمية كبيرة في ذلك الوقت. وكان الحل الذي اتبعه الجيش الألماني لهذه المشكلة هو استخدام تقنية كانت تعتبر حديثة جدًا في ذلك الوقت، ألا وهي تقنية الراديو (اللاسلكي) لبث الأوامر من قيادة الجيش إلى الوحدات في الميدان مباشرة.

وفي واحدة من السوابق الأولى المسجلة لما يُسمى الآن «استخبارات الاتصالات» (SIGINT) أو (Signals Intelligence) بدأ الجيشان الإنجليزي والفرنسي في الاستفادة من الفارق المهم بين نظام البرق التقليدي ونظام البرق اللاسلكي، فاختراق خط برقي لاسلكي يتطلب تدخلاً بشريًا مما يعني أخطارًا كبيرة ربما تؤدي إلى اكتشاف المقتحم والقبض عليه، أما اختراق خطوط الاتصالات اللاسلكية فإنه لا يحتاج إلى تدخل بشري وإنما يتطلب موارد فنية وهوائي ضخم (مثل برج إيفل الشهير بباريس). وقد أمكن في

تلك الفترة كسر معظم الشفرات المستخدمة لبساطتها وبدائيتها، وبذلك كثيرًا ما كانت خطط الهجوم الألمانية تقع في أيدي قوات الحلفاء قبل أن تصل هذه الخطط إلى الوحدات المكلفة بتنفيذها في جبهة القتال.

في مجال جمع المعلومات من الطبيعي أن تلجأ أجهزة المخابرات إلى الأساليب التي تتميز بقلة فرص اكتشافها وبانخفاض تكلفتها وارتفاع درجة الثقة في معلوماتها، وفي مجال الشبكات وإنترنت بالذات فكل ما هو مطلوب لبناء وحدة لاستخبارات الاتصالات (SIGINT) هو جهاز حاسب شخصي لالتقاط المعلومات ثم توصيله بالشبكة المطلوب اقتحامها، ولما كانت معظم الاتصالات التي تتم بين حاسبات أي شبكة مغلقة تكون في العادة غير مشفرة فإن اتصال الجهاز المقتحم بالشبكة يتيح له الوصول لجميع المعلومات التي تمر عبر كوابل هذه الشبكة بحرية تامة.

هذه المخاوف، برغم واقعيتها، إلا أنها لا يجب أن تُترك لتنمو حتى تخلق لدى الإدارة العليا في المنظمات المختلفة خوفًا لا مبرر له من الارتباط بشبكة إنترنت، فهذه الشبكة تعتبر موردًا في غاية الأهمية له العديد من الفوائد الإيجابية لكافة المنظمات على اختلاف أهدافها، والمهم أن تظل أعيننا مفتوحة على الأخطار المحتملة وأن نعرف كيف يمكن التغلب عليها. ولكن كثيرًا ما يكون علينا أن نوازن بين مستوى الأمن وسهولة الاستخدام، ويكمن التحدي الحقيقي في كيفية الوصول إلى درجة أمن كافية دون أن نجعل نظام المعلومات غير عملي أو صعب الاستخدام.

٤ . ٢ التجسس الصناعي

ربما كانت مجرد المشاهدة لبعض التطبيقات أو البرامج كافية لنقل التقنية (أو اقتباس التقنية) بما يخل بحقوق الملكية الفكرية، فلم يحتج «ستيف

جوبز» (أحد الصديقين اللذين أخرجا كمبيوتر آبل إلى الوجود) إلا لمجرد مشاهدة واجهة المستفيد (GUI) التي تستخدم الرسوم والأيقونات بمركز أبحاث (بالو آلتو) في شركة زيروكس في عام ١٩٧٢ . ويقول مدير المركز (Xerox,1999) أن ستيف جوبز بمجرد رؤيته هذه الواجهة وقعت الخسارة بالفعل، فيكفي أنه عرف أن هذا الأمر يمكن تنفيذه.

٤ . ٢ . ١ خسائر الشركات البريطانية بسبب خرق قواعد السلامة والأمن في نظم معالجة المعلومات

أشار تقرير صدر عن وزارة التجارة والصناعة البريطانية تحت عنوان «الأمن المعلوماتي»، ونشرته وكالات الأنباء العربية في أغسطس ١٩٩٩، إلى ازدياد نسبة الشركات التي تعرضت لخرق قواعد الأمن فيها إلى ٤٥ في المائة عام ١٩٩٨ بالمقارنة مع ٣٦ في المائة عام ١٩٩٤ . وتتراوح أنواع الخرق بين سطو اللصوص على مركبات وعناصر الكومبيوترات أو أجهزة الحاسب نفسها، وبين عدم اهتمام العاملين بأخذ نسخة احتياطية من المعلومات الهامة، هذا فضلاً عن حوادث التسلل والاحتيال.

ومع ازدياد تدفق المعلومات وتنوع مصادرها وتوسع التجارة الإلكترونية عبر الإنترنت تتحول الكثير من مصادر المعلومات إلى وسائط يسهل اختراقها، مما يؤدي إلى ضرورة وضع نظم حماية خاصة بها وزيادة تكاليف الأمن والحماية. ويشمل ذلك حماية المعلومات داخل الأقراص الصلبة في أجهزة الحاسب، والبريد الإلكتروني وأجهزة الفاكس ونظم تسجيل المعلومات الصوتية، بالإضافة إلى حماية شبكات نقل البيانات.

٤ . ٢ . ٢ جرائم نظم المعلومات في الشركات الصغيرة

جرائم نظم المعلومات تجدها بجميع (المقاسات) والأشكال بدءًا من قيام موظف باستخدام الحاسب في طباعة خطاب شخصي وانتهاء بمدير كبير يهرب بالملايين، وربما كانت الشركات الصغيرة والمصالح الحكومية من بين أكثر الجهات تعرضًا لجرائم نظم المعلومات، ربما كان ذلك بسبب بعض الخصائص التي تميز الشركات الصغيرة مثل: الاعتماد المتزايد على الحاسب الآلي وقلة الضوابط والاحتياطات الأمنية وصعوبة فصل المهام خاصة في ظل قلة عدد الموظفين، الاتجاه إلى استعمال إجراءات غير رسمية، وجود درجة عالية من الثقة المتبادلة بين صاحب الشركة وموظفيه. وأحيانًا تجد الشركات الصغيرة أنه من الصعب أن تقوم بتطبيق نفس إجراءات الأمن الخاصة بالمؤسسات الكبيرة فبعض هذه الإجراءات لا يصلح إلا مع الحجم الكبير للموارد والعدد الكبير من الموظفين، ففي الشركات الصغيرة من المعتاد أن ترى شخصًا واحدًا مسئولاً عن تشغيل الحاسب وعادة يكون موضع الثقة الكاملة، ومع معرفته الكاملة بالتفاصيل الفنية عن تشغيل الحاسب والصلاحيات اللازمة لذلك فإن هذا يفتح الباب على مصراعيه لارتكاب الجريمة.

وقد فتحت شبكة الإنترنت الباب واسعًا أمام جريمة الكمبيوتر، فقد رحب المجرمون كثيرًا بما تتيحه لهم الشبكة من إخفاء لشخصياتهم عند التعامل مع الآخرين، وربما كان إبقاء الشخصية مجهولة مهمًا جدًا حتى بين المتواطئين أنفسهم فهو يعفيهم من أمور كثيرة هم في غنى عنها.

٤ . ٢ . ٣ إحدى جرائم الشركات الصغيرة

كان «جو» هو المبرمج الوحيد في أحد البنوك الصغيرة في كاليفورنيا، كما كان هو مشغل الكمبيوتر أيضًا، وكان مظهره متواضعًا جدًا ولكنه كان

عبقريًا في مجال الكمبيوتر وكان قادرًا على حل أي مشكلة في هذا المجال. وكان «جو» يعاني من بعض المشاكل المالية وعندما تفاقمت هذه المشاكل وازدادت ديونه قرر أن يقوم بعملية خاطفة على البنك الذي يعمل به بالتواطؤ مع صديقة له.

أتى «جو» إلى العمل مبكرًا ذات يوم وقام بتشغيل الكمبيوتر ثم قام بتعديل تاريخ اليوم في الحاسب وبعد ذلك قام بتحويل مبلغ ٤٠ ألف دولار من حساب أحد المودعين إلى حساب صديقته، ثم قام بتمزيق التقرير المطبوع عن هذه العملية وإزالة السجل الرقابي الإلكتروني الذي يتم تسجيله آليًا عن مثل هذه العمليات، ثم أعاد تاريخ اليوم في الحاسب مرة أخرى إلى اليوم الصحيح. ولكن لسوء حظه قام العميل بالصدفة بالاستفسار عن حسابه قبل أن تقوم صديقته بسحب المبلغ. وهكذا تم القبض على «جو».

فيما بعد اعترف رئيس البنك أنه كان عليه أن يشك في سلوك المبرمج الموثوق به بعد أن شاهد سيارته الجديدة الفاخرة وجهاز الاستريو غالي الثمن الذي اقتناه والشقة الفاخرة التي اشتراها في إحدى ضواحي المدينة، ولكنه برر سكوته عن كل ذلك بأنه لم يكن يريد أن يغضب المبرمج الوحيد في البنك والذي يعتمد عليه كثيرًا والذي كان يستطيع أداء أي مهمة للبنك طالما كان مزاجه معتدلاً!.

في الواقع فهناك أكثر من «جو» في المؤسسات الصغيرة يسرقون الأموال أو البضائع، والفرصة أكبر لظهورهم في المؤسسات الصغيرة عن تلك الكبيرة التي يوجد فيها موظفون كثيرون وتتم فيها عمليات فصل المهام وازدواج الضوابط بشكل أكثر حزمًا.

٤ . ٣ التجسس التجاري

التجسس هو نشاط قديم قدم البشرية، واليوم يزداد هذا النشاط انتشارًا وتوسعًا، فلم يعد قاصرًا على الشئون العسكرية أو على زمن الحرب، فكثير من الحكومات الآن تمارس التجسس على الأعمال التجارية في دول أخرى دعمًا لمصالحها التجارية. وهي تقوم بذلك علنًا ودون أدنى محاولة من جانبها لإخفاء ذلك، ومثال ذلك أنشطة التجسس التي مارستها الحكومة الفرنسية ضد شركة «ا. ب. م.».

في عام ١٩٩٦ أُجري استفتاء بين مسئولية الأمن الصناعي في الشركات الأمريكية أظهر أن كثيرًا من الدول قد حصلت بشكل غير مشروع على معلومات سرية عن أنشطة تجارية وصناعية في الولايات المتحدة. وتم ترتيب هذه الدول وفقًا لحجم الانتهاكات على النحو التالي: الصين، كندا، فرنسا، الهند، اليابان، ألمانيا، كوريا الجنوبية، كمنولث الدول المستقلة (الاتحاد السوفييتي السابق)، تايوان، المملكة المتحدة، إسرائيل، المكسيك، باكستان، سنغافورة، هونج كونج (*ASIS,1998*).

بالمقابل فإن الولايات المتحدة لا تقل اهتمامًا بالتجسس التجاري على الآخرين، والمعلومات المنشورة عن التجسس التجاري الدولي نادرة، فالدول والشركات لا تعترف في العادة بقيامها بهذا النوع من التجسس، أو هي حتى لا تعترف بوقوعها ضحية له.

ونذكر فيما يلي بعض الوسائل التي أصبحت تُستخدم الآن بكثرة في التجسس التجاري الدولي:

- إغراء بعض من لديهم المعلومات على البوح بها (سواء بمقابل أو بدون).
- الاستفادة من الشراكة التجارية بين الدول ومن الأبحاث المشتركة، أو بشراء بعض المكونات الحساسة من الشركات الصانعة لها.
- استثارة النزعات الدينية أو العرقية أو المذهبية أو السياسية للموظفين للحصول منهم على المعلومات سواء بالترغيب أو بالترهيب.
- استخدام أساليب أبحاث التسويق لجمع المعلومات عن المنافسين واستخدام الاستمارات التي يقوم بملئها طالبو الوظائف أو إخفاء بعض الأسئلة غير البريئة ضمن الاستبيانات.
- جمع المعلومات الاستخباراتية من المعارض العامة والمؤتمرات والرحلات السياحية والنوادي والمطاعم.
- شراء المعلومات من الأفراد، بما في ذلك سماسرة المعلومات الذين يتكسبون من التجسس وبيع المعلومات.
- استضافة الزوار الأجانب في دول أخرى والحصول منهم على المعلومات المطلوبة في مقابل إكرام وفادتهم وتمويل زيارتهم لهذه الدولة وتجولهم فيها.

وتعمد بعض الحكومات إلى استئجار بعض المقتحمين لأجهزة الكمبيوتر لمساعدتها في التجسس التجاري. ويحكي «كليفورد ستول» في كتابه الشهير «بيضة الديك أنه قد حدث في ألمانيا أن حاول بعض ممثلي الحكومات الأجنبية الاتصال ببعض الأشخاص المشهور عنهم هواية اقتحام أجهزة الكمبيوتر، وقد تم القبض عليهم إثر قيامهم باقتحام شبكة نظم المعلومات الخاصة بحكومة الولايات المتحدة لنقل بعض المعلومات إلى عملاء روس (Stoll).

٤ . ٤ أساليب جديدة للتجسس

من الأساليب المستحدثة للتجسس الإلكتروني على نظم المعلومات أسلوب (إخفاء المعلومات داخل المعلومات) وبرغم صعوبته أحيانًا إلا أنه غير نادر الحدوث في جرائم المعلومات، ويتميز هذا الأسلوب بأن الكشف عن المعلومات المخفاة أمر صعب إن لم يكن مستحيلاً في بعض الأحيان.

في هذا الأسلوب قد يلجأ المجرم إلى إخفاء بعض المعلومات الحساسة داخل معلومات أخرى عادية داخل الحاسب، ثم يلجأ إلى وسيلة لتسريب المعلومات العادية (الحاوية) من هذا الحاسب، فلا يشك أحد في أن هناك معلومات حساسة يجرى تسريبها. فالجاسوس يخاطر كثيرًا إذا لجأ إلى طباعة المعلومات التي يخطط لسرقتها أو حاول عرضها على شاشة الحاسب لأن الضحية قد يلحظ هذه التصرفات ويوقفها، أو قد يقوم الحاسب بتسجيل هذه المحاولات (Logging). ولذلك يلجأ الجواسيس إلى وسائل غير تقليدية للحصول على المعلومات السرية، فقد يقوم الجاسوس مثلاً بكتابة برنامج وتنفيذه خلسة على حاسب الضحية حيث يفحص هذا البرنامج كل البيانات المخزنة على الحاسب ثم يومض أحد المصابيح الصغيرة الموجودة على لوحة الحاسب لفترة قصيرة إذا كان البيان (٠) أو يومض لفترة أطول إذا كان البيان (١)، ثم يقوم الجاسوس بتسجيل شريط فيديو لهذه اللوحة عن طريق تسليط كاميرا فيديو (مخفية بمهارة) على لوحة الحاسب لتسجيل عمليات الوميض المتتالية. وبإدارة هذا الشريط بعد ذلك ببطء يمكن قراءة البيانات المسجلة في الحاسب دون ترك أثر ينم عن الجاسوس.

ويلجأ بعض الجواسيس إلى طرق مشابهة لأسلوب الفيديو ولكن بدلاً من تسجيل الوميض المتقطع فيقومون بطباعة بيانات تبدو عادية بحيث يرمز

السطر الكامل إلى الرقم (١) والسطر غير الكامل إلى الرقم (٠). أو أن يتم تصوير حركة شريط ممغنط خلال دورانه بحيث تمثل الدورة الكاملة للشريط الرقم (١) بينما تمثل نصف الدورة الرقم (٠)، أو يستخدمون الصوت الصادر عن آلة الطباعة لتمثيل الأصفار والآحاد، أو يستقبلون موجات راديو تنبعث من وحدة بسيطة (Diode) يتم تركيبها خلسة في دائرة الحاسب لكشف هذه البيانات. وهذه الأساليب تتم بالطبع بالنسبة للبيانات التي تتميز بصغر الحجم وعظم الأهمية.

ويلجأ جواسيس آخرون لطرق أقل تعقيدًا برشوة بعض المشغلين أو عمال النظافة للحصول على مخرجات الحاسب بدلاً من إعدامها، وسنطرق هذا الموضوع فيما تبقى من هذا الفصل عند حديثنا عن التواطؤ وأهميته في جرائم نظم المعلومات.

٤ . ٥ أثر التواطؤ في جرائم نظم المعلومات

من المعلوم لكل خبراء أمن المعلومات أن من أفضل وسائل مكافحة الجريمة هو أن نجعل التواطؤ ضروريًا لنجاح ارتكابها، أي ضرورة تعاون أكثر من شخص، ويزيد ذلك من تعقيد الجريمة كما يزيد من فرص اكتشاف المجرمين.

وفي جرائم نظم المعلومات تزداد أهمية التواطؤ إذ أنه لا يوجد عادة شخص واحد لديه كل المهارات المطلوبة والمعارف اللازمة بالإضافة إلى الصلاحيات الضرورية لإنجاح الجريمة. وبعد وضع الضوابط والإجراءات الأمنية موضع التنفيذ تكون فرصة ارتكاب جرائم نظم المعلومات محصورة في الموظفين ذوي الصلاحيات العالية (وهم يكونون بالطبع موضع الثقة الكاملة) والذين لا يخضعون عادة إلا للقليل من الضوابط

والإجراءات. هؤلاء الموظفون لابد لهم من التعاون مع متخصصي الكمبيوتر حتى يمكنهم تنفيذ جريمة نظم المعلومات. وهؤلاء المتخصصون يمكنهم تجاوز الضوابط والقيود الفنية الموضوعة لحماية المعلومات أو لتسهيل ضبط مرتكب الجريمة، بينما الموظفون ذوو الصلاحيات العالية فيكون دورهم هو تقديم الصلاحيات الضرورية للوصول إلى المعلومة.

ولكي يستطيع خبراء أمن المعلومات مواجهة هذا التواطؤ المحتمل فإنهم يعملون على حث الإدارة على تفعيل الضوابط التي تعنى بالعامل البشري أو الإنساني مثل (الفصل بين المهام) و (تعدد الضوابط). ويستطيع الكمبيوتر المساعدة بشكل فعال في هذه الضوابط، فيمكن مثلاً أن يطلب الكمبيوتر من المستخدم تحديد شخصيته والتحقق منها بشكل آلي، كما يمكن أن يطلب الحاسب إجراء مستقلاً يؤديه أكثر من موظف لتنفيذ العملية كأن يقوم موظف الشباك في البنك بإدخال قيمة المبلغ بينما يلزم اعتماد مراقب البنك للعمليات ذات المبالغ الكبيرة، كما يمكن للحاسب كذلك أن يراجع آليًا ملف تسجيل الوقائع لاكتشاف أي عملية مريبة.

وقد أفادت عدة تقارير (Parker,1998) بأن هناك نسبة من التواطؤ في جرائم نظم المعلومات في المؤسسات الكبيرة أكبر بكثير منها في المؤسسات الصغيرة، وأن التواطؤ شائع الحدوث بصفة عامة في هذا النوع من الجرائم.

في إحدى الوقائع قام رئيس شركة تجارية كبرى بتزوير الإيرادات الحقيقية للشركة تفاديًا لدفع الضرائب المستحقة على مبلغ ١٦ مليون دولار، وذلك بأن زود شركته بنظامين منفصلين تمامًا للمحاسبة يستخدم كل منهما كمبيوتر مستقل، وقد احتاج لإتمام خطته لمساعدة بعض المشغلين لتنظيم هذه العملية المعقدة التي تضمن تشغيل نظام مزدوج لمسك الدفاتر لأنه ليست لديه المعرفة الفنية الكافية لتنفيذ ذلك.

وفي واقعة أخرى تمكن سكرتير مسئول تحويل الأموال في شركة أوروبية كبرى من التقاط كلمة المرور الخاصة برئيسه خلال إدخالها للحاسب من لوحة المفاتيح، وباستخدام هذه الكلمة بالإضافة إلى كلمة المرور الخاصة به قام بمحاولة احتيال لنقل أكثر من ٥٠٥ مليون دولار إلى حساب شريكه في المؤامرة في لوزان بسويسرا، ولفت انتباه أحد موظفي البنك في لوزان ضخامة المبلغ المحول فقام بإبلاغ المركز الرئيسي للبنك طالبًا الموافقة على هذا التحويل. وكانت هذه هي بداية الخيط الذي أدى في النهاية إلى تمكن الشركة من الإمساك بالمجرم، وبسؤاله عما دعاه إلى القيام بهذا العمل ادعى (وهو عضو في جماعة دينية متطرفة) أن الله أمره بأن يفعل ذلك! ويقضي هذا السكرتير الآن عقوبة طويلة في السجن. بعد هذا الحادث أضافت الشركة الأوروبية عددًا من الضوابط الأمنية والتي تضمنت الفصل الصارم بين المهام للحد من إمكان التواطؤ المتعمد أو غير المتعمد، وكذلك إعادة هندسة إجراءات مراقبة عمليات الحاسب لجعل إخفاء مثل هذه الجريمة أكثر صعوبة في المستقبل.

أما أكبر عملية نصب مالية في أوروبا فقد حدثت عندما قام بعض كبار التجار بالتعاون مع بعض متخصصي الحاسب الآلي بإخفاء معاملاتهم داخل نظم الحاسب الآلي وفي بعض الوسائط الإلكترونية، وتمكنت هذه العصابة من اختلاس ما قيمته ٢٦٠ مليون دولار. أما قضية التأمين الخاصة بشركة (EFI) التي سبق ذكرها في هذا الفصل فقد احتاج إتمامها إلى تواطؤ ٢٢ شخصًا على الأقل بدءًا من رئيس الشركة إلى مجموعة من مشغلي الحاسب الآلي.

الفصل الخامس
الأخطار التي تواجه الإنترنت

٥ . ١ الأمان في شبكة الإنترنت

٥ . ٢ الأخطار الشائعة على الشبكة .

٥ . ٣ تصنيف المشكلات الأمنية على الشبكة .

الأخطار التي تواجه الإنترنت

نحاول في هذا الفصل الإجابة عن السؤال الذي يتردد على ألسنة الكثيرين هذه الأيام وهو : هل شبكة الإنترنت شبكة آمنة؟ فنتحدث عن مدى أمن الشبكة ، ثم نتحدث عن أكثر الأخطار شيوعًا على الشبكة مثل التطفل وإفشاء الأسرار والتلاعب والسرقة ، ثم نختتم هذا الفصل بمحاولة تصنيف المشكلات الأمنية على الشبكة وذلك تمهيدًا للفصل القادم الذي خصصناه لجرائم الإنترنت باعتبارها أحدث وأخطر جرائم نظم المعلومات الآن .

٥ . ١ الأمان في شبكة الإنترنت

لا شك أن التقنيات الحديثة في العصر الإلكتروني الذي نعيشه الآن ونحن على مشارف القرن الحادي والعشرين ، وبخاصة شبكة الإنترنت ، قد كثفت من عمليات انتهاك الشبكات . بل إن هذه التقنيات جعلت من الممكن أن يتم هذا الانتهاك بشكل آلي ، فنحن نرى الآن بعض البرامج (Crawls) التي تجوب شبكة الإنترنت آليًا على مدار الساعة بحثًا عن المواقع الجديدة وحصرها وتسجيلها وتحديد كل وافد جديد على الشبكة .

هذه التقنيات شجعت وساعدت المجرمين على زيادة عدد وحجم جرائمهم دون زيادة في الجهد المبذول عما كانوا يبذلونه مع الوسائل التقليدية ، بل مع انخفاض احتمالات انكشاف أمرهم .

وتسمح الشبكات للمجرمين بأن يرتكبوا جرائمهم بعيدًا عن مسرح الجريمة ، كما تسمح لهم بمهاجمة أكثر من ضحية في الوقت الواحد (ربما آلاف الضحايا في حالة الفيروسات) . فلصوص بطاقات الائتمان مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت ، ومن ثم بيع هذه المعلومات للآخرين .

وأنت بمجرد أن تصل جهاز الحاسب الشخصي لديك بشبكة الهاتف العمومية، وحتى قبل الدخول على الإنترنت فإنه، على الأقل من الناحية النظرية، يستطيع أي شخص استخدام هذا الحاسب. فشبكة الإنترنت للأسف ليست شبكة آمنة بأي حال.

ويساعد بقاء شخصية مستخدم الإنترنت مجهولة على ارتكاب جرائم المعلومات من جانب الإرهابيين ومروجي الجنس، ويشجع كذلك على جرائم النصب والاحتيال وعمليات القمار وغيرها. وسنبين في الفصل القادم كيف يخفي المجرم شخصيته على شبكة الإنترنت.

٥ . ٢ الأخطار الشائعة على الشبكة

هناك العديد من الأخطار التي تنشأ عن الارتباط بشبكة إنترنت، وعند تحليلنا لهذه الأخطار يجب أن نركز على الثغرات التي قد ينجم عنها العديد من التهديدات للمعلومات، وكلما زادت كمية التهديدات التي قد تنتج عن ثغرة ما، وكلما زادت درجة خطورة هذه التهديدات على المنظمة زادت بالتالي حتمية وضرورة محاولة إغلاق هذه الثغرة بكل الوسائل.

ويجب ألا نعتني فقط بتلك الأخطار التي قد ينتج عنها خسائر مالية، وإنما يجب أن نتعدى ذلك إلى ما يهدد الخطط الإستراتيجية للمنظمة.

ومن المهم ألا نغفل مدى واقعية هذه التهديدات، فالتهديدات التي يصعب أن تتحقق سواء لاحتياجها إلى تقنيات عالية أو خبرة كبيرة من جانب المقتحم، ومن ثم يكون احتمال حدوثها محدودًا، لا يجب أن نوليها نفس الاهتمام الذي نوليه للتهديدات التي يكون احتمال حدوثها كبيرًا.

ويمكن تصنيف الأخطار التي تواجه المنظمة التي ترتبط بهذه الشبكة على النحو التالي :

٥ . ٢ . ١ التطفل

التعرض للتطفل من جانب الآخرين أمر لا يمكن تجنبه على الشبكة ، وفي بعض المواقع يصبح هذا الأمر جزءًا من الروتين اليومي للمسئولين عن هذه المواقع . فبمجرد الانضمام للشبكة يصبح العضو الجديد مرئيًا من جانب ملايين المشتركين الآخرين . فلا تحتاج «مجسات العناوين» Address Probes تلك البرمجيات المتحفزة على مدار الساعة ، سوى لبضع دقائق قليلة حتى تكتشف وجود أي موقع جديد أو جهاز جديد دخل حديثًا إلى الشبكة . هذا الانكشاف أمام العالم كله يعني أن المنظمات لا يكفيها الاعتماد على الأمن المادي أو البيئة الآمنة التي تحكم السيطرة عليها لتتأكد من أن معلوماتها في أمان ، كما أن هذه المنظمات لا يجب أن تطمئن كثيرًا لحاجز المسافة التي تفصلها عن العدو لتتأكد من أن معلوماتها أبعد من أن تُطال !

في الماضي كانت المعلومات المحظورة يتم حجبها بواسطة نظم متعددة ، ما زال بعضها يستخدم حتى الآن وبكفاءة لا بأس بها ، أما الآن فتتعدد الأخطار التي تتعرض لها معلومات المستفيدين على الشبكة وربما كان أكثر هذه الأخطار شيوعًا ، وإن كان أقلها ضررًا ، هو حب الاستطلاع أو الفضول الذي يقود البشر إلى التجول والإبحار في فضاء الإنترنت . هذا الفضول الذي يلازم البشر منذ بدء الخليقة والذي يرجع إليه الفضل في معظم ، إن لم يكن في جميع ، الاختراعات والاكتشافات العلمية والجغرافية .

٥ . ٢ . ٢ التجسس الإلكتروني والإرهاب

أما التجسس الإلكتروني والإرهاب، سواء تم من جانب المنافسين التجاريين أو بواسطة مجموعات تحركها دوافع سياسية، فإنه يعتبر أحد التهديدات الخطيرة الواردة في عصرنا هذا والتي يجب أن يحسب حسابها. ومع تقدم التقنية ظهرت وسائل حديثة متقدمة لمقاومة هذه الأخطار وعلينا ألا نتردد في استخدامها.

٥ . ٢ . ٣ تهديد الخصوصية

وتشكل خصوصية المعلومات عاملاً إضافيًا يثير القلق، فقوانين احترام الخصوصية في عالمنا العربي ليست صارمة بما فيه الكفاية، هذا إن وجدت أصلاً. وإفشاء الأسرار الحساسة للأفراد سواء الشخصية أو المهنية أو الصحية أو المالية أصبح الآن مخاطرة ليست بعيدة الاحتمال.

والفشل في اتخاذ احتياطات أمنية كافية في عالم اليوم، الذي يزيد فيه ترابط العالم أو قل تشابك العالم قد تنتج عنه آثار قانونية خطيرة خلال السنوات القليلة القادمة، فيوجد حاليًا في الولايات المتحدة عدة قضايا تعويضات بملايين الدولارات يتم تداولها في المحاكم ضد بعض وحدات الرعاية الصحية بسبب إفشاء معلومات من الملفات الطبية لبعض مرضاهم (Hutt,1995).

٥ . ٢ . ٤ إفشاء الأسرار

هذا هو أكثر المحاذير التي تخشى منها الكثير من المنظمات التي تود الارتباط بشبكة إنترنت، فالمنظمة إذا عانت من إفشاء متكرر لمعلوماتها الحساسة فربما انعكس ذلك بشكل خطير على أرباحها أو صورتها العامة أو الاثنتين معًا، فمعرفة الموقف التفاوضي أو التنافسي للمنظمة يسمح للطرف المنافس بخفض الأسعار مثلاً، أو بزيادة أرباحه على حساب هذه المنظمة.

٥ . ٢ . ٥ التلاعب

تأخذ عملية التلاعب بالبيانات أشكالاً عديدة مختلفة، وكثيرًا ما يكون المتسبب فيها من العاملين بالمنظمة نفسها، فالمعلومات التي تحتفظ بها المنظمة يمكن تغييرها أو تزويرها. والدوافع لذلك متعددة بعضها قد يكون عملاً عدائيًا مباشرًا ضد المنظمة يهدف لإلحاق الضرر بها، أو قد يكون عملاً غير مباشر دوافعه تحقيق مصالح منظمات أخرى.

٥ . ٢ . ٦ السرقة

السرقة باستخدام الحاسب على شبكة إنترنت قد تحدث نتيجة اختراق لنظام محلي أو إقحام عملية مزورة تصل من خلال الشبكة. والسرقة يمكن أن تقع على بعض المعلومات الحيوية المحظورة التي يمكن إفشاؤها أو بيعها في مقابل مادي، أو قد تقع السرقة على أصول أخرى ذات قيمة مثل أرقام بطاقات الائتمان التي يمكن أن تُستغل لسحب مبالغ مالية من رصيد صاحب البطاقة. ومفتاح الحماية ضد السرقة والمعاملات المزورة هو استخدام التقنيات المناسبة لفرز الرسائل المستقبلة ومنع الضار منها.

٥ . ٣ تصنيف المشكلات الأمنية على الشبكة

يمكن تقسيم مشكلة الأمن إلى ثلاث مشكلات فرعية:

٥ . ٣ . ١ أمن المعاملات التجارية

وهو الأمن المفقود، والذي زادت حدة المخاوف من آثاره بازدياد استخدام الشبكة والاعتماد عليها في أمرين:

٥ . ٣ . ١ . ١ «التجارة الإلكترونية» (Electronic Commerce)

هذه هي المشكلة الأولى، حيث يتم من خلال الشبكة تبادل المعلومات

التجارية بين الشركات، كما يتم كذلك تبادل عروض الشراء وأوامر التوريد والمعلومات حول أسعار الأسهم والسندات واتجاهات السوق وغير ذلك من المعلومات فائقة الأهمية والحساسية، والأمن هنا تكمن خطورته في أنه يتعلق بالأسرار التجارية للشركات وخططها الاستراتيجية ومواقفها المالية، بل دعنا نقل أنه قد يتعلق باقتصاديات الدول.

٥ . ٣ . ١ . ٢ «التسوق الإلكتروني» (Electronic Shopping)

أما المشكلة الثانية في أمن المعاملات التجارية فنتجت عما نطلق عليه «التسوق الإلكتروني» (Electronic Shopping) أو «السوق الإلكترونية» (Electronic Market)، حيث يرسل العملاء رقم بطاقة الائتمان الخاصة بهم «فيزا» أو «ماستر كارد» عبر الشبكة إلى الشركة التي تقدم الخدمة أو تبيع السلعة للحصول على هذه السلعة. ولا يستطيع العميل أن يضمن عدم وقوع هذه المعلومات في يد أخرى (طرف ثالث) قد يستغلها بشكل سيئ.

ويزداد الاتجاه الآن إلى التشفير (التعمية) كحل لهذه المشكلة، وهناك أساليب عديدة لتشفير الرسائل المتبادلة في هذا المجال والحفاظ على سريتها ولكنها مكلفة وليست مضمونة مائة بالمائة.

٥ . ٣ . ٢ أمن المعلومات المحفوظة في قواعد البيانات

لما كانت قواعد البيانات الآن مفتوحة عبر الشبكة لاستخدام مستخدمي الشبكة من كافة أنحاء العالم، فهناك دائمًا خطر إساءة استخدام هذه المعلومات أو إمكان اختراق حواجز السرية الموضوعة على هذه البيانات. والسوابق في هذا الموضوع كثيرة، والمحاولات المتكررة لاختراق قواعد البيانات في جهات أمنية على أعلى درجة من السرية والخطورة مثل وزارة الدفاع الأمريكية ليست بعيدة وليست فريدة أو غير متكررة.

وبدأ مؤخرًا الالتفات بشدة واهتمام إلى هذه الظاهرة ومحاولة علاجها عن طريق استخدام نظم قوية لأمن البيانات وضوابط الدخول إلى قواعد المعلومات .

٥ . ٣ . ٣ جرائم الحاسب

المعلومات خلال وجودها داخل الحاسب لا تحتاج إلا إلى إجراءات أمنية محدودة ، أما خلال رحلتها من حاسب إلى آخر فالمخاطر كثيرة ، فالرحلة طويلة ومحفوفة بالمخاطر في جميع مراحلها ، فالكابل الذي تمر فيه نبضات المعلومات يحتاج إلى تأمين ، وشبكة الهاتف العامة غير آمنة تمامًا ، وشبكة الإنترنت ربما كانت أطول المراحل زمنًا وأقلها أمنًا ، ومن هنا اكتسبت الحماية باستخدام التشفير أهميتها في حالة البيانات المنقولة ، ولعل التشفير هو أفضل وسيلة عملية لتأمين البيانات خلال رحلتها خارج جدران غرفة الحاسب .

وقبل عصر الشبكات كانت جرائم الحاسب محدودة لأن مرتكبها كان من الضروري أن يكون متواجدًا في مركز الحاسب ، أما الآن وبعد انتشار الشبكات أصبح من الممكن ارتكاب جريمة تزوير في أحد بنوك الرياض مثلاً من أقصى الأرض ، فالشبكات جعلت ارتكاب جرائم الحاسب مثل التزوير والاختلاس أو انتهاك الخصوصية أو تدمير المعلومات أو سرقتها أكثر سهولة . بل إن هناك بعض الكتب التي تشرح كيفية ارتكاب هذه الجرائم ، وهناك بعض المواقع على شبكة إنترنت تشرح كيف يمكن اختراق حواجز السرية ، أو كيف يمكن إدخال الفيروسات عنوة إلى الحاسبات المحصنة ! .

السادس

جرائم الإنترنت

٦ . ١ الهجوم على مواقع الإنترنت .

٦ . ٢ انتحال شخصية الأفراد .

٦ . ٣ انتحال شخصية المواقع .

٦ . ٤ الجنس الفاضح على الإنترنت .

٦ . ٥ الإغراق بالرسائل .

جرائم الإنترنت

نخصص هذا الفصل لتقديم بعض الجرائم التي اشتهرت بها شبكة الإنترنت بعد أن مهدنا لها في الفصل السابق للأخطار التي تهدد الشبكة ومشاكلها الأمنية، وسنستمر في الفصول القادمة في تغطية جرائم الإنترنت. نبدأ هذا الفصل بالحديث عن الهجوم على مواقع الإنترنت وتعرض بعض المواقع الحصينة والخطيرة لهذا الهجوم، وعن انتحال شخصية الأفراد على الشبكة وكيف ينفذها المجرمون، وعن انتحال شخصية المواقع وكيف تتم، ثم نتحدث باختصار شديد عن الجنس الفاضح على شبكة الإنترنت.

٦ . ١ الهجوم على مواقع الإنترنت

يعتبر الهجوم على المواقع المختلفة في شبكة الإنترنت (اقتحام المواقع) من الجرائم الشائعة في العالم. وقد تعرضت لهذا النوع من الجرائم في الولايات المتحدة مثلاً كل من وزارة العدل والمخابرات المركزية والقوات الجوية، كما تعرض له حزب العمال البريطاني.

وفي مثل هذا النوع من الهجوم كثيرًا ما يكون الضرر محدودًا كأن يقوم المهاجم بوضع صورة خليعة على هذا الموقع (مثلما حدث عند وضع صورة زعيمة أحد الأحزاب الاسترالية الشهيرة في وضع مخجل في موقع الحزب على الشبكة)، أو تعديل بعض العناوين من باب السخرية (مثلما حدث عندما أنشأت إحدى شركات أمن المعلومات موقعًا لها على شبكة الإنترنت لترويج لمنتجاتها من برامج وأجهزة أمن المعلومات ووضعت عنوانًا لموقعها عبارة (We are always UP) فقام أحد المقتحمين بالدخول على الموقع وغير

هذا العنوان ليصبح (We are always DOWN)، وأعتقد أن نجاح هذه الشركة قد تأثر بشكل كبير بهذا العمل.

هذه الأعمال التي تبدو تافهة وغير مؤذية تؤدي إلى إضعاف الثقة في صحة بيانات هذه المواقع، وبرغم أن المسئولين عن هذه المواقع قد اعتادوا على إزالة آثار هذه العمليات، إلا أنه في بعض الأحيان قد يكون الضرر أخطر، فقد يقوم المجرم بتعديل المعلومات على الموقع كأن يقوم بتعديل أسعار السلع أو إقحام بعض الإعلانات عن بضائع وهمية غير مقدمة في هذا الموقع.

٦ . ٢ انتحال شخصية الأفراد

المقصود بانتحال الشخصية ما يعمد إليه المجرم من استخدام شخصية شخص آخر للاستفادة من سمعته مثلاً أو ماله أو صلاحياته. ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الإنترنت.

ومنتحل الشخصية يمكنه استخدام بعض المعلومات التي يمكن الحصول عليها بسهولة من الإنترنت، مثل الاسم والعنوان ورقم الهوية مثلاً، وأحيانًا يكون ذلك كافيًا لانتحال شخصية شخص آخر.

ونجد هذه الأيام الكثير من الإعلانات المشبوهة على الإنترنت، فقبل كتابتي هذه السطور بدقائق اطلعت على رسالة واردة بالبريد الإلكتروني تعلن عن «كاميرا» فاخرة شبه مجانية سوف تُرسل إلي بالبريد بمجرد ملء بعض البيانات البسيطة مثل الاسم والعنوان و(رقم بطاقة الائتمان) لدفع نصف دولار تبرعًا لمرضى السرطان من الأطفال، وأن هذا هو كل المطلوب مني لأتلقى الكاميرا الفاخرة خالصة أجور البريد والتغليف والشحن!!

وبالطبع لم أقع في هذا الفخ الساذج وإن كنت لا أستبعد أن يكون آخرون قد وقعوا فيه .

ورغم أن انتحال الشخصية جريمة قديمة وليست قاصرة على نظم المعلومات أو الإنترنت ، إلا أن تغلغل شبكة الإنترنت في عالمنا (أو قل تغلغلنا فيها) قد زاد بشكل واسع من مقدرة اللصوص على جمع المعلومات الشخصية المطلوبة عن الضحية واستخدامها في جرائمهم .

يمكن أن تؤدي جريمة انتحال الشخصية المعلوماتية إلى استنزاف رصيد الضحية في البنك أو السحب من بطاقته الائتمانية أو الإساءة إلى سمعة الضحية . وقد يرتكب المجرم جريمة النصب على الآخرين مستغلاً الشخصية المنتحلة للضحية ، مستفيدًا من السمعة الطيبة لشخص ما أو شركة قد تكون استغرقت السنوات الطوال لبناء هذه السمعة . وكثيرًا ما نرى كيف أن بعض المجرمين يعمدون إلى تغيير العنوان البريدي للضحية إلى عنوان المجرم لكي يستقبل بنفسه الفواتير والمطالبات التي قد تنبه الضحية إلى أن شيئًا مريبًا يحدث .

وذكرت الصحف قصة امرأة من كاليفورنيا تعرضت لعملة انتحال الشخصية من جانب أحد المجرمين (فعلى الإنترنت لا يشترط أن يتنكر الرجل في زي امرأة لكي ينتحل شخصيتها) ، وبعد القبض على المجرم لم تتمكن الضحية من الحضور إلى المحكمة للإدلاء بشهادتها لأن المحكمة أرسلت لها الاستدعاء على عنوان المجرم وليس على عنوانها هي ! .

في كثير من الحالات تقوم البنوك بتعويض الضحايا من عملائهم الذين يتعرضون لعمليات انتحال الشخصية عن الأموال التي فقدوها ، أما فقد السمعة أو الحرج أو الوقت المهدر في محاولة إثبات البراءة أو جهود استعادة السمعة ، فلن تعوض البنوك عنها شيئًا .

٦ . ٢ . ١ إخفاء الشخصية على الإنترنت

أحيانًا يحتاج مجرم الإنترنت لإخفاء شخصيته خلال العملية التي يقوم بها، فعند إرسال خطاب تهديد بالبريد العادي لا يضع المجرم عنوانه على المظروف، ولكن شبكة الإنترنت بها نظام آلي يضع عنوان المرسل في مقدمة كل أجزاء الرسالة المرسلة عبر الشبكة . وبالتالي يجب على المجرم أن يتجاوز هذا النظام بتغيير عنوان المصدر لبروتوكول الإنترنت (IP) الذي يظهر في مقدمة أجزاء الرسالة ليستبدل به عنوانًا آخر مغلوطًا بحيث يصبح تتبع المصدر الأصلي للرسالة عملية صعبة أو مستحيلة (Cohen,1996) . ويُطلق على هذه العمليات اسم (IP Spoofing) . وأحيانًا يختار المجرم عنوانًا لجهاز حاسب يستطيع الوصول إليه واستخدامه حتى يستطيع معرفة رد فعل الضحية ومدى استجابته للتهديد مثلاً (Dunnigan,1995) .

ولحسن الحظ فإن أي تعديل في بروتوكولات الاتصال بشبكة الإنترنت أو استخدام توقيع طرف ثالث يجعل عملية إخفاء الشخصية تزداد صعوبة يومًا بعد يوم .

٦ . ٢ . ٢ انتحال الشخصية عبر البريد الإلكتروني

تزييف رسائل البريد الإلكتروني لتبدو صادرة من شخص آخر هو أمر شائع الحدوث على شبكة الإنترنت، وبرغم أن الكثير من هذه الرسائل ليست مؤذية وتمر على سبيل الفكاهة، إلا أن بعضها الآخر يكون شديد الأذى .

والاتساع الهائل لشبكة إنترنت وعدم إمكان التعرف بسهولة على الشخصية الحقيقية لمرسل البريد الإلكتروني يتطلب أن يتم فحص المعلومات المارة عبر الشبكة للتأكد من شخصية مرسلها وعنوانه، وأكثر الوسائل كفاءة

لتحقيق ذلك هو اللجوء إلى طرف ثالث مستقل وموثوق به. هذا الطرف الثالث يُسمى «سلطات الإجازة» (CA) أو (Certificate Authorities) والتي يمكن من خلالها الحصول على «التوقيع الرقمي» و«العنوان الرقمي» وإتمام تشفير الاتصالات. وتتحقق سلطات الإجازة من شخصية المستفيدين وتجيزها عن طريق تبادل بعض المعلومات الشخصية التي لا يعرفها إلا الطرفان (السلطة المجيزة والمستفيد المجاز). كما تقوم سلطات الإجازة بتسجيل الرسائل المتبادلة للتحقق منها لاحقًا، كما تستخدم بعض برمجيات التحقق لتتبع مصدر الرسائل والتأكد من صحة المصدر.

ويلزم التنبيه إلى أن سلطات الإجازة ليست مضمونة مائة بالمائة، فإذا كان لدى المجرم الوسيلة للوصول إلى الحاسب الشخصي الخاص بالمستفيد الحقيقي، وكانت لديه المعلومات الكافية لاستخدام كلمة المرور الصحيحة، فإنه يستطيع خداع سلطات الإجازة وينتحل شخصية المستفيد الحقيقي.

يتطلب حل هذه المشكلة فصل عملية التحقق من شخصية المستفيد عن عملية التحقق من الجهاز الذي يستخدمه، ويتم ذلك عن طريق استخدام رقم خاص وأجهزة محمولة لتحقيق الشخصية «توكن» (Token) والتي يحملها المستفيد معه باستمرار، وبذلك لا يستطيع منتحل الشخصية استخدام الحاسب بدون استخدام جهاز تحقيق الشخصية المحمول. والفكرة هنا هي أننا نتحقق من شخصية المستفيد بالتأكد مما يعرفه (كلمة مرور مثلاً)، والتأكد في نفس الوقت مما لديه (جهاز تحقيق الشخصية المحمول).

٦ . ٢ . ٣ مثال عن انتحال شخصية عبر البريد الإلكتروني

القصة التي نوردها هنا حدثت في ولاية كاليفورنيا عام ١٩٩٦ وهي قصة فتاة متوسطة العمر كانت صديقة للمدير التنفيذي لإحدى الشركات

الكبرى المتخصصة في البرمجيات، ولما هجرها صديقها الكبير وفُصلت من الشركة رفعت الفتاة دعوى الفصل التعسفي على الشركة، وكسبت القضية وحصلت على تعويض قدره مائة ألف دولار. قبل فصلها كانت هذه الفتاة هي المساعدة الأولى لنائب رئيس الشركة، وكانت هي المسئولة عن تغيير كلمات المرور الخاصة برئيسها! بحيث تعطيه باستمرار الرمز الجديد في كل مرة، كما أنها كانت تتولى متابعة بريده الإلكتروني والرد على رسائله.

وكان الدليل الرئيسي الذي قدمته الفتاة للمحكمة في قضية الفصل التعسفي هو نسخة من رسالة واردة بالبريد الإلكتروني ادعت هذه الفتاة أن رئيسها (نائب رئيس الشركة) قام بإرسالها إلى المدير التنفيذي للشركة يقول فيها «لقد قمت بفصل (آدلين) بناء على طلبك». ولكن المدير التنفيذي أنكر أنه قد فصل المرأة بسبب رفضها إقامة علاقة معه مؤكدًا أن رسالة البريد الإلكتروني هي رسالة مدسوسة.

بعد انتهاء القضية والحكم للفتاة بالتعويض، أنكرت الشركة في عام ١٩٩٧ صحة الرسالة المزعومة، وبناء على ذلك قام المدعي العام بتوجيه الاتهام ومحاكمة الفتاة بالتهم التالية: اقتحام شبكة الحاسب، وصنع وثيقة زائفة، والحنث باليمين أمام المحكمة العليا. وقد قدمت الشركة سجلات مراقبة الحاسب التي تبين أن شخصًا ما قد دخل إلى الحاسب (Logon) من موقع بعيد ليس من داخل الشركة باسم نائب الرئيس، ثم انتقل إلى اسم شخص آخر وظل يتنقل بين رقم المستفيد الخاص بنائب الرئيس والرقم الخاص بهذا الشخص الآخر عدة مرات في نفس اليوم والساعة التي أُرسلت فيها الرسالة موضوع التحقيق. وأثبت نائب الرئيس أنه كان يقود سيارته ويجري بعض المحادثات من خلال هاتفه الجوال في اللحظة التي أُرسلت فيها رسالة البريد الإلكتروني. ولم يتمكن المحققون من استعادة آخر بيانات

تم إدخالها من الحاسب الشخصي الخاص بالفتاة، إذ أنها قد مسحت كل هذه البيانات، وبرغم ذلك فقد أُدينت الفتاة وحُكم عليها بقضاء عام في السجن وغرامة قدرها مائة ألف دولار.

٦ . ٣ انتحال شخصية المواقع

يعتبر أسلوب انتحال شخصية المواقع على شبكة الإنترنت (Web Spoofing) من الأساليب الحديثة نسبيًا في عالم جرائم نظم المعلومات، ولكنه أشد خطورة وأكثر صعوبة في اكتشافه من أسلوب إخفاء الشخصية (IP Spoofing)، ومن المتوقع أن يكثر استخدام هذا الأسلوب في جرائم نظم المعلومات في المستقبل. ولتنفيذ هذه الجريمة يستفيد المجرم من حقيقة أن أي كمبيوتر على الإنترنت يمكن أن يقحم نفسه في موقع بيني بين البرنامج المستعرض (Browser) للحاسب الخاص بأحد مستخدمي الإنترنت وبين الموقع (Web). ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي، ويستطيع مراقبة أي معلومات متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه، كما يستطيع سرقة هذه المعلومات أو تغييرها، وتمتد هذه الثغرة إلى برامج استعراض المواقع الحالية الشهيرة.

والخطير في الأمر أن عملية انتحال شخصية المواقع يمكن تنفيذها حتى لو تم الاتصال بالموقع من خلال نظم الاتصال الآمنة (أو التي تبدو آمنة)، وكثير من المواقع تدعي أنها تتصل بالمستفيد من خلال «خادم آمن» (Secured Server) وتضع رمز (القفل) الذي يشير إلى أمن الاتصال، ولكن أسلوب انتحال شخصية المواقع في مقدوره اختراق هذا الحاجز.

٦ . ٣ . ١ كيف يرتكب المقتحم هذه الجريمة؟

ولكي يشن المجرم هجومًا من هذا النوع فهو يحتاج إلى السيطرة على أحد المواقع التي تتم زيارتها بكثرة، ثم يقوم بتحويله ليعمل كموقع بيني، وتحتاج عملية التحويل هذه إلى مهارة خاصة في برمجة المواقع (Web programming)، أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك. وبمجرد أن يكتب مستخدم الإنترنت اسم هذا الموقع فإنه يقع في المصيدة ويدخل إلى شبكة العنكبوت (لا شبكة الإنترنت)، أي إلى الموقع المشبوه الذي أعده المجرم لاصطياد زبائنه، فالمجرم قد غير أحد الروابط (Links) التي تؤدي إلى بعض المواقع الشهيرة ليجعلها تؤدي إلى موقعه المشبوه، وهكذا يصبح موقع المجرم في الوسط بين المستفيد والموقع الشهير، ويستطيع من هذا الموقع المتوسط أن يتلصص على المعلومات التي يتم تبادلها بين المستفيد والموقع الشهير.

والحل الوحيد الذي يجعل المستفيد يفلت من هذه المصيدة آمنًا هو أن ينتقل مباشرة إلى عنوان موقع معروف آمن بالضغط مثلاً على أحد الأزرار أو الأيقونات التي تؤدي إليها.

٦ . ٣ . ٢ ما يجب أن تنتبه إليه أجهزة الخدمة في المواقع

للأسف فإن الأسلوب التي تستخدمه أجهزة الخدمة في المواقع (Web Servers) لترجمة عناوين المواقع المطلوب دخول المستفيد إليها يسهل من عملية انتحال المواقع ويجعلها ممكنة. فمستخدمي البرامج المستعرضة (Browsers) ينتقلون من موقع إلى آخر عن طريق سلسلة من العناوين يقود كل منها إلى الآخر، حتى يصلون إلى العنوان الأخير في السلسلة. وبالتالي

فإذا نقر المستفيد على أيقونة معينة للدخول إلى موقع إحدى الشركات وليكن مثلاً : (www.Company.com) ، وكان العنوان (URL) المرتبط بهذه الأيقونة مكتوبًا على النحو التالي :

(www.evil.com/http://www.Company.com) فإن خادم الموقع سوف يصل هذا المستفيد بالعنوان (www.Company.com)، الذي يريده ولكن الاتصالات كلها سوف تتم من خلال العنوان (www.evil.com).

والملاحظ أن بعض أجهزة الخدمة في المواقع عند استقبالها مثل هذا العنوان المركب فإنها سوف تعرض للمستفيد رسالة خطأ وترفض تنفيذ الاتصال، ولكن أجهزة الخدمة المهيأة بحيث تفك سلسلة العناوين وتتعامل معها سوف تنفذ المطلوب دون رسالة خطأ ويقع المستفيدون المرتبطون بها في الفخ وتمر كل بياناتهم بالموقع (www.evil.com) .

ويستطيع مستخدمو هذا الأسلوب أن يجعلوا من الصعب جدًا على الضحية اكتشاف الخدعة باستخدام برامج بلغة «جافا سكربت» (Java Script) لعرض صفحات الموقع على المستعرض (Browser)، ولكن مع إخفاء وجود الموقع المتوسط المشبوه.

والطريقة الوحيدة المؤكدة التي يستطيع بها المستفيد اكتشاف وجود الموقع المشبوه هي أن يراجع تعليمات المصدر المكتوبة بلغة (HTML) أو بلغة «جافا سكربت» للتأكد من العنوان الحقيقي وأنه لا وجود لمواقع متوسطة.

ولأن عملية انتحال المواقع هي عملية من الصعب اكتشافها، فإن المجرمين يمكنهم استخدام هذا الأسلوب لسرقة أو تعديل المعلومات السرية للضحية دون مخاطرة تذكر بالانكشاف، ويمكن أن يستمر ذلك لعدة أيام أو ربما أسابيع.

٦ . ٣ . ٣ نصائح عند الدخول إلى موقع على الإنترنت

يجب على مستخدمي المواقع الالتزام بالنصائح التالية لحماية أنفسهم من عملية انتحال المواقع :

- تأكد من أن السطر الذي يحمل العنوان في البرنامج المستعرض مرئي بوضوح ، وتأكد من أنه يشير إلى الموقع المقصود .
- أخرج من البرنامج المستعرض بمجرد أن تنتفي الحاجة إلى بقائك به ، ويمكنك العودة إليه مرة أخرى عند الحاجة . فإن ذلك يقلل من الوقت المتاح للموقع المشبوه لكي يظل على اتصال بك .
- استخدم «علامة المكان» (Bookmark) لزيارة المواقع عندما تنوي التعامل مع بيانات سرية أو خاصة .
- راجع العناوين في ملفات «علامة المكان» بصفة دورية للتأكد من أنها لا تشير إلى مواقع متوسطة .
- لا توافق على تمكين برامج «جافا» و«جافا سكربت» و«آكتف إكس» إلا عند الضرورة فهي تسهل عملية انتحال المواقع .

٦ . ٣ . ٤ مثال على عملية انتحال المواقع

يوضح المثال التالي كيفية انتحال المواقع بحيث يصبح الموقع المشبوه متوسطًا بين موقع المستفيد والموقع الذي يريد الاتصال به :

عندما يزور المستفيد من خلال البرنامج المستعرض موقعًا على الإنترنت فإنه عادة يكتب عنوانًا مثل : (www.Company.com) ، ومن الممكن أن يحدث خطأ من جانب المستفيد في كتابة أحد الحروف دون قصد ، فيكتب اسم الموقع هكذا : (www.C0mpany.com) بكتابة صفر بدلاً من حرف (o) ،

فماذا لو كان هناك موقع باسم (C0mpany) موجودًا بالفعل؟ يمكن للمجرم أن يعد موقعه بحيث يقلد الموقع الأصلي وتكون له نفس الواجهة ونفس الشكل، وسيبقى موقعه هذا متوسطًا بين المستفيد والموقع الحقيقي المقصود. وعندما يطلب المستفيد اتصالاً (آمنًا) بالموقع فإن موقع المجرم يمكنه أن يجهز مثل هذا الاتصال ولكن مرورًا بموقعه المشبوه.

٦ . ٤ الجنس الفاضح على الإنترنت

سوف نتحدث هنا باختصار شديد عن الجنس الفاضح على شبكة الإنترنت. وسبب الاختصار هو أننا نود أن نتجنب الاستفاضة في هذا الموضوع أو إعطاء أمثلة للمواقع سيئة السمعة التي تشتهر بهذا النوع من الجرائم الخلقية، فكثيرًا ما يؤدي ذلك إلى نتيجة عكسية.

تتيح شبكة الإنترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ. وما يُطلق عليه «جنس الأطفال» هو من أخطر هذه الممارسات في الوقت الحالي.

٦ . ٥ الإغراق بالرسائل

تتم عملية الإغراق بالرسائل (Spamming)، وهي تعتبر من جرائم نظم المعلومات، عن طريق إرسال عشرات الرسائل من البريد الإلكتروني لشخص ما أو للعديد من مستخدمي الإنترنت.

وقد بدأت هذه العملية في عام ١٩٩٦ عندما أرسلت إحدى الشركات إعلانات عنها بالبريد الإلكتروني إلى الآلاف من مواقع الإنترنت، وفضلاً

عن تعطيل الشبكة الذي نجم عن هذا الإغراق فقد تكلف متلقو هذه الرسائل الكثير في استقبالها ودفع ثمن مدة الاتصال اللازمة لاستقبال هذه الرسائل مع ما يصاحبها من ملفات. ويقع ضحية لهذه الجريمة أيضًا مقدمو خدمة الإنترنت حيث يتم ملء منافذ الاتصال (Communication ports) وقوائم الانتظار (Queues) لأجهزة الخدمة الخاصة بهم، وينتج عن ذلك انقطاع الخدمة عن زبائنهم.

وتجرى حاليًا محاولات من جانب شركات نظم المعلومات لتطوير برامج تتعامل مع هذه الحالات باستقبال جزء محدود من الرسائل عندما يحدث سيل مفاجئ منها حتى لا تنقطع الخدمة.

الفصل السابع

أمن البريد الإلكتروني

٧ . ١ أهمية أمن البريد الإلكتروني .

٧ . ٢ المستفيد وأمن البريد الإلكتروني .

٧ . ٣ الاحتياجات الأمنية للبريد الإلكتروني .

٧ . ٤ استراتيجيات تأمين البريد الإلكتروني .

٧ . ٥ التقنيات الحديثة لتأمين البريد الإلكتروني .

٧ . ٦ بوابة التشفير .

٧ . ٧ اختيار أسلوب حماية البريد الإلكتروني .

أمن البريد الإلكتروني

أنشأ التطور المستمر والمتلاحق في تقنيات المعلومات بعض الآثار الجانبية السلبية من أهمها أثره على أمن البريد الإلكتروني، ونتعرض في هذا الفصل لأثر الانتشار الكبير لشبكات المعلومات وازدياد الاعتماد على البريد الإلكتروني كوسيلة اتصال لا غنى عنها في نشوء مشكلة المحافظة على أمن البريد الإلكتروني. كما نتعرض للمخاطر الأمنية التي تحيط بالبريد الإلكتروني خلال رحلته من المرسل إلى المستقبل ومعايير الأمن التي يجب أن تؤخذ في الاعتبار عند اقتناء نظام للبريد الإلكتروني. ثم نتطرق للاستراتيجيات المختلفة المتبعة حاليًا لتأمين البريد الإلكتروني ونقارن بينها، ثم نستعرض التقنيات المستخدمة حاليًا لتأمين البريد الإلكتروني وهي تقنيات تشفير الرسائل، والقيم الاختبارية، والتوقيع الرقمي، وكيف تتضافر هذه التقنيات فيما يسمى بالغلاف الرقمي للرسالة أو صندوق الشفرة المغلق لتحقيق أمن البريد الإلكتروني. وفي النهاية نبين كيفية اختيار الأسلوب المناسب لمواجهة كل من الأخطار الرئيسية التي يتعرض لها البريد الإلكتروني.

٧ . ١ أهمية أمن البريد الإلكتروني

٧ . ١ . ١ انتشار البريد الإلكتروني

أصبح البريد الإلكتروني الآن وسيلة اتصال لا غنى عنها في الكثير من مجالات العمل، خاصة في الاتصالات الثنائية، فقد بدأ يقترب في شيوعه وانتشاره من الهاتف لدرجة أن كثيرًا من الموظفين في الشركات المختلفة يستخدمونه في تبادل المعلومات. وهذه المعلومات قد تكون في غاية الحساسية مثل خطط الشركة المستقبلية أو الأسعار التي تنوي الشركة أن تبيع

بها منتجاتها أو الحد الأقصى للخصم الذي تمنحه لعملائها أو استراتيجيات البيع لدى الشركة ، أو ربما المعلومات الفنية الخاصة بالتصنيع ، إلى غير ذلك من المعلومات الهامة .

لذلك لم يكن غريبًا أن تستهدف صناعة أمن المعلومات البريد الإلكتروني بالذات كمجال للاهتمام به والعمل على تأمينه ، بل وتشجيع العملاء على تبني تقنيات أمن المعلومات . ودافعهم إلى ذلك هو تنامي أهمية البريد الإلكتروني وتزايد حجم استخدامه في كثير من الشركات والمؤسسات إلى جانب معرفة صناع تقنيات أمن المعلومات بأنه على الرغم من ذلك فإن مستخدمي البريد الإلكتروني لا يأخذون قضية الأمن بالجدية اللازمة ، بل يكتفون باستخدام كلمات السر في الدخول إلى الحاسب كوسيلة تأمين، وهي بالقطع ليست وسيلة تأمين مثالية، هذا في الوقت الذي أصبحت فيه إجراءات تأمين البريد الإلكتروني سهلة وممكنة وتقنياته متاحة ومتوفرة ، مثال لذلك تقنيات التشفير المختلفة وتقنيات المفاتيح المستخدمة فيه وحوائط النار وغير ذلك.

٧ . ١ . ٢ تزايد المخاطر الأمنية المحيطة بالبريد الإلكتروني

كلما ازداد انتشار البريد الإلكتروني وازداد اعتماد الجميع عليه ازدادت المخاطر الأمنية التي تحيط به، ومع تزايد كم المعلومات المنقولة عبر الشبكات المحلية وعبر شبكة إنترنت على وجه الخصوص يصبح مسار هذه المعلومات محفوفًا بالكثير من المخاطر الأمنية. والسهولة التي يمكن بها تزييف البريد الإلكتروني تجعل عملية تأمينه أكثر صعوبة، فالمرسل يمكن تزييف شخصيته ومحتويات البريد نفسها يمكن تعديلها، كل ذلك دون ترك أي أثر أو دليل. علاوة على ذلك فلا توجد، إلى حد ما، وسيلة للسيطرة على المسار

الذي يسلكه البريد الإلكتروني خلال رحلته عبر الشبكة، وهذه وحدها ثغرة حقيقية في جدار أمن المعلومات.

٧ . ٢ المستفيد وأمن البريد الإلكتروني

٧ . ٢ . ١ نظرة المستفيد إلى أهمية تأمين البريد الإلكتروني

تتداول الصحف والدوريات العلمية الآن أنباء كثيرة عن الاختراقات الأمنية المتعددة في أماكن كثيرة من العالم ليس آخرها اختراق أجهزة الحاسب في البنتاجون (وزارة الدفاع الأمريكية)، وقد لاقت هذه الأنباء اهتمامًا كبيرًا لدى القيادات العليا في المؤسسات، ومن ثم بدأت هذه القيادات تحرص على تطبيق إجراءات أمنية كافية تعفيهم من الحرج الذي وقع فيه الآخرون، ولكننا نرى المستفيد العادي في المؤسسة على العكس من ذلك يجنح إلى رفض إجراءات السرية الصارمة والقيود البوليسية التي توضع على استخدام الملفات وقواعد البيانات والبريد الإلكتروني، ويردد كثير من المستفيدين قولهم: «ليس لدينا شيء نخفيه»، وهذا الاتجاه قد يكون مدمرًا في أحوال معينة وفي مجالات معينة، ومن المؤكد أن كثيرًا من مستخدمي البريد الإلكتروني لم يلفت انتباههم أحد إلى سهولة تطفل الآخرين على بريدهم وما يمكن أن يترتب على ذلك.

يختلف مدى اقتناع الإدارة العليا في المؤسسات بأهمية البريد الإلكتروني وأهمية تأمين استخدامه من مؤسسة لأخرى، ويتوقف ذلك على طبيعة عمل المؤسسة نفسها، ومدى الخطر الذي تعتقد المؤسسة أنها قد تتعرض له في حالة تعرض بريدها الإلكتروني للخطر. وربما كان العامل الحاسم في مدى أهمية أو عدم أهمية تأمين البريد الإلكتروني هو محتويات

هذا البريد وهل هي مجرد مكاتبات روتينية أم أنه يحتوي على خطط سرية أو معلومات محظورة.

٧ . ٢ . ٢ الحاجة إلى بريد إلكتروني آمن

إذا بحثنا عن العملاء الذين يحتاجون إلى بريد إلكتروني آمن نجدهم منتشرين في قطاعات واسعة من الأعمال، فأهل الصناعة يرسلون ويستقبلون بانتظام كميات كبيرة من المعلومات عن التصميمات التي يتم إنتاجها بواسطة الحاسب في صورة بريد إلكتروني، ويتبادلون هذه المعلومات بين مواقع العمل المختلفة بحيث يقوم الفنيون بإعداد التصميمات الجديدة ثم إرسالها إلى المصانع لكي تستخدم في الإنتاج عن طريق تحميلها مباشرة في ذاكرة الآلة التي تتم إدارتها بواسطة الحاسب. وخلال الرحلة التي تقطعها هذه التصميمات من مكان لآخر تكون عرضة للتخريب أو السرقة، ولذلك يتعين حمايتها، بل إن هذه المعلومات يجب أيضًا حمايتها حتى وهي موجودة في ذاكرة الحاسب ولو لم تنتقل إلى أي مكان، ومن هنا أتى اهتمام الشركات بأساليب التشفير المختلفة كما سنذكر فيما بعد.

ونجد كذلك الشركات التجارية وتنامي ما يطلق عليه الآن «التجارة الإلكترونية» (Electronic Commerce)، حيث يستخدم البريد الإلكتروني كبديل كامل عن المكاتبات الورقية بين شركات الجملة وعملائها من شركات التجزئة. والتسوق الإلكتروني أيضًا هو أحد المجالات الفعالة للبريد الإلكتروني حيث يستخدمه الناس لطلب البضائع والاشتراك في الدوريات وذلك عن طريق ذكر بيانات البطاقة الائتمانية (مثل بطاقة «فيزا» أو «ماستر كارد»)، وهنا مثلاً نجد لأمن البريد الإلكتروني دورًا هامًا يلعبه في حماية المستهلك، وبالإضافة إلى كل ذلك هناك بالطبع العديد من المجالات التي تحتاج إلى بريد إلكتروني آمن.

٧ . ٣ الاحتياجات الأمنية للبريد الإلكتروني

٧ . ٣ . ١ معايير أمن البريد الإلكتروني

عند قيام الأفراد أو الشركات أو متخصصي الشبكات أو مسئولي الأمن بالمؤسسات بدراسة وتحديد احتياجاتهم من أمن البريد الإلكتروني عليهم وضع المعايير التالية في الاعتبار :

٧ . ٣ . ١ . ١ سلامة محتويات الرسالة

لا يبالي معظم الناس بمحاولة تعديل محتويات الخطاب البريدي لصعوبة ذلك (برغم عدم استحالته)، ولكن الأمر يختلف في حالة الوسط الإلكتروني، فعلى طول مسار الشبكة يمكن اختراق هذه الشبكة وتعديل محتويات الرسالة الإلكترونية دون ترك بصمات أو آثار أو أقفال محطمة. ولذلك تعين وجود آلية ما للتأكد من أن (ما أرسله الطرف المرسل هو ما استقبله الطرف المستقبل).

٧ . ٣ . ١ . ٢ التحقق من شخصية المرسل وتوثيق الرسالة

برغم أن الاحتياطات التي تتخذ في حالة البريد العادي مثل استخدام نموذج الخطابات المطبوع، ووجود التوقيعات في أسفله، والأختام الرسمية التي تعززه، والغلاف المغلق بإحكام، هي كلها أمور يمكن تقليدها، إلا أنها تعتبر وسائل مقبولة للتحقق من الشخصية وعدم التزوير. أما البريد الإلكتروني فهو أكثر سهولة في التزوير، ولذلك فإن المستفيدين يكونون دائمًا في حاجة إلى التأكد من أن الرسالة حقيقية، أو أن (ما تم إرساله صادر فعلاً عن المرسل الحقيقي)، وأن هذا (المرسل لا يستطيع إنكار إرساله للرسالة). وبذلك يمكن استخدام رسائل البريد الإلكتروني كوثائق رسمية.

٧ . ٣ . ١ . ٣ الحفاظ على الخصوصية ومنع سرقة الرسائل أو التطفل عليها

إرسال البريد العادي في مظروف مغلق معنون باسم المرسل إليه يحقق الخصوصية، ولكن لا يوجد النظير المقابل في حالة البريد الإلكتروني، فإرسال البريد الإلكتروني الذي يفتقر إلى الحماية أشبه بإرسال بطاقة بريدية يمكن قراءتها في أية نقطة خلال رحلة البريد وبواسطة أي شخص.

وكلما ازداد حجم المعلومات المتبادلة بين الناس عبر شبكات المعلومات فهناك فرصة متزايدة لاطلاع أشخاص غير مصرح لهم على هذه المعلومات أو تعديلها أو حتى فقدها بالكامل. والتقارير الكثيرة التي تمتلئ بها الدوريات المتخصصة تبعث على القلق وتجعل المسئولين في الشركات على اختلاف مستوياتهم غير مطمئنين بشأن حماية معلوماتهم المتبادلة.

٧ . ٣ . ٢ متطلبات نظم أمن البريد الإلكتروني

هناك بعض الشروط التي يجب توفرها في نظم الأمن التي تستخدم لتأمين البريد الإلكتروني وهي:

- أن تكون مرنة بحيث يكون من الممكن تغيير نطاق استخدامها، فيمكن أن تستخدم داخل قسم معين في المؤسسة أو أن تستخدم على نطاق المؤسسة بأكملها، ولكل نطاق تشغيل بالطبع احتياجاته الخاصة وأساليبه المختلفة في التطبيق.
- أن تعتمد نظم البريد الإلكتروني ونظم التشفير المصاحبة لها على أنظمة من نوع «الخادم والمخدوم» (Client/Server) بحيث يكون للمخدومين جميعًا «مراسم» (Protocols) متشابهة، فإن ذلك يزيد من سرعة تبادل الاتصالات فيما بينهم دون الانتقاص من أمن المعلومات المتبادلة.

- أن تكون هذه النظم قادرة على التعامل مع أي جهاز أو برمجية لدى المستفيدين على اختلاف أنواع هذه الأجهزة أو البرمجيات.
- أن تكون برمجيات البريد الإلكتروني مجهزة بنظم التشفير، إذ أن ذلك يعفي المؤسسات من استحداث أساليب تشفير خاصة بها تستنزف الوقت والمال.
- أن تكون سهلة الاستخدام من جانب المستفيد فإن لم تكن كذلك فلن يستخدمها هذا المستفيد، فلا يجب أن يزيد مجهود المستخدم عن مجرد النقر على أيقونة معينة ليتم تشفير الرسالة أو فك تشفيرها، وشيء مشابه لذلك للتحقق من شخصية المرسل (التوقيع الرقمي كما سيأتي ذكره).

٧ . ٤ استراتيجيات تأمين البريد الإلكتروني

توجد في الوقت الحالي استراتيجيتان أساسيتان لتأمين البريد الإلكتروني، ولتوضيح الفرق بينهما نشبه تأمين البريد الإلكتروني بمحاولة تأمين الطريق السريعة من دخول الجمال والحيوانات إليها، فنحن إما أن نقوم بحماية الطريق ذاتها بوضع سياج على جانبيها وإما أن نقوم بتقييد الحيوانات والسيطرة عليها لمنعها من الوصول إلى الطريق. ويقابل هذا المثال في تأمين البريد الإلكتروني استراتيجيتان هما تأمين الشبكة أو تأمين الرسائل نفسها.

في البداية عادة ما تتبع الشركات الاستراتيجية الأولى (تأمين الشبكة)، ويتم ذلك عن طريق تركيب برمجيات «جدران النار» (Fire Walls)، وتأمين مركز الحاسب تأمينًا ماديًا، ولكن تقييد استخدام البيانات أو الوصول إليها لا يكون فعالاً إلا عندما تكون هذه البيانات قابعة في مكان واحد، بينما نجد أن معظم البيانات الآن دائمة الحركة والانتقال والتبادل عبر المدينة الواحدة ومن مدينة إلى أخرى، بل عبر الكرة الأرضية كلها في بعض

الأحيان. ولذلك هناك شركات كثيرة تجد أن هذا الحل البسيط المتمثل في حماية الشبكة فقط ليس كافيًا لتحقيق الأهداف الأمنية الأربعة التي يجب توفرها في البريد الإلكتروني الآمن وهي:

- خصوصية الرسائل بحيث لا يتم الاطلاع عليها إلا بواسطة المرسل إليه وحده.
- جعل النجاح في تعديل الرسائل أمرًا مستحيلاً.
- أن يكون مستقبل الرسالة قادرًا على التحقق من شخصية المرسل.
- ألا يكون مرسل الرسالة قادرًا على إنكار قيامه بإرسالها.

للوصول إلى هذا المستوى من الأمن للبريد الإلكتروني اتجهت شركات عديدة إلى الحل الثاني وهو تأمين الرسائل نفسها وليس تأمين الشبكة (أو تقييد الحيوانات ومنعها من التسلل إلى الطريق).

ونرى أن تأمين البريد الإلكتروني لكي يكون فعالاً فلابد من المزج بين الاستراتيجيتين أخذًا بمفهوم الأمن الشامل بحيث يتم تأمين الشبكة وتأمين الرسالة معًا.

٧ . ٥ التقنيات الحديثة لتأمين البريد الإلكتروني

هناك شبه إجماع بين الشركات المنتجة للنظم الأمنية حول التقنيات المستخدمة فيها، فجميع الأساليب المستخدمة لتأمين البريد الإلكتروني تعتمد على تقنيات التشفير والتوقيعات الرقمية، بينما تختلف هذه الشركات فيما بينها في طريقة التنفيذ فقط وليس في المبادئ الأساسية.

٧ . ٥ . ١ تشفير البريد الإلكتروني

التشفير هو أهم وسائل تأمين البريد الإلكتروني على الإطلاق،

والتشفير على نوعين إما أن يكون تشفيرًا «متماثلاً» (Symmetric) يستخدم أسلوب «المفتاح السري» (Private Key) أو أن يكون تشفيرًا «غير متماثل» (Asymmetric) يستخدم أسلوب «المفتاح العلني» (Public Key).

٧ . ٥ . ١ . ١ التشفير المتماثل

يستخدم في هذا الأسلوب مفتاح سري «وحيد» (unique)، وهذا المفتاح يستخدم في عملية تشفير الرسائل أو فك شفرتها. فالطرفان اللذان يودان تبادل رسائل مؤمنة يجب عليهما استخدام نفس المفاتيح، كما يجب عليهما كذلك الاحتفاظ بهذه المفاتيح سرية فيتبادلان هذه المفاتيح بطريقة تضمن عدم اطلاع طرف ثالث عليها.

٧ . ٥ . ١ . ٢ التشفير غير المتماثل

يستخدم في هذا الأسلوب زوج من المفاتيح، أحدهما يكون علنيًا أي يكون معلومًا لأكثر من شخص ويتم تبادله بين الأطراف المختلفة، أما المفتاح الآخر فيظل سريًا لا يعرفه سوى طرف واحد (صاحب المفتاح). وإذا تم تشفير الرسالة بواسطة أحد المفتاحين فإن فك شفرتها يحتاج إلى استخدام المفتاح الآخر، فإذا تم تشفير الرسالة وإرسالها باستخدام المفتاح العلني للطرف الذي أرسلت له الرسالة (الطرف المستقبل) مثلاً فلا يمكن فك شفرتها إلا باستخدام المفتاح السري لهذا الطرف، ويناسب هذا الأسلوب طبيعة الرسائل التي يتم إرسالها إلى جهة واحدة محددة. أما إذا كان المطلوب إرسال رسالة مشفرة إلى عدة جهات فيلزم أن يستخدم في تشفيرها المفتاح السري للطرف المرسل بحيث يمكن لأي جهة من الجهات المعنية باستقبال الرسالة فك شفرتها باستخدام المفتاح العلني للطرف المرسل والذي يكون متوفرًا لديها.

ويعتبر استخدام تقنية « التشفير باستخدام المفتاح العلني» (Public Key Encryption) هو الحل الأفضل ، حتى الآن ، الذي يتيح الأمن والسلامة المطلوبين للمعلومات ، كما أنه يحتفظ في الوقت نفسه بشخصية المرسل وبالتالي يمكن التحقق منها وضمان عدم إنكار المرسل صدور الرسالة عنه . فمن الأساسيات التي يفترض أن تكون متوافرة في جميع برمجيات البريد الإلكتروني الآن أن تقوم بالتأكد من شخصية المرسل وأن تضمن أنه من غير الممكن لأي شخص أن يقوم بتزوير الرسالة أو نسبتها إلى مصدر آخر ، فالبرنامج لدى الطرف المرسل عليه أن يقوم بتشفير الرسالة وتوقيعها قبل إرسالها ، بينما على البرنامج الموجود لدى الطرف المستقبل أن يقوم بفك شفرة الرسالة والتأكد من صحة التوقيع . هذه الإجراءات قد ينتج عنها بعض التأخير في وصول الرسالة بسبب عمليتي التشفير وفك الشفرة ، إلا أنه من الناحية العملية فإن ذلك لن يتسبب في أي تأخير محسوس ، وهذا النوع من البرمجيات أصبح الآن متاحًا بالفعل في الأسواق .

تُستخدم تقنية « التشفير باستخدام المفتاح العلني» (PKE) عادة داخل المؤسسة نفسها أو بينها وبين بعض المؤسسات الأخرى التي تتعامل معها ، وتضمن هذه التقنية تأمين الاتصالات عبر شبكة إنترنت التي اشتهرت بسوء السمعة فيما يتعلق بتسرب المعلومات والافتقار إلى الأمن . وتلجأ بعض الشركات الآن إلى استخدام نفس النسخ من برمجيات البريد الإلكتروني لديها ولدى عملائها في الوقت نفسه ، وكذلك الأمر بالنسبة لنظم التشفير وبذلك يمكن تأمين كافة الاتصالات بين الشركة وعملائها .

٧ . ٥ . ٢ القيم الاختبارية

تقوم نظم التشفير بإنشاء ما يسمى بالقيم «الاختبارية» (Hash values) ، وهذه القيم الاختبارية هي مجموعة من الحروف يتم استخلاصها عن طريق

معالجة البيانات المطلوب إرسالها بواسطة دوال معينة، وهذه القيم تكون ثابتة الطول مهما اختلف حجم البيانات التي استخلصت منها. فلو كانت الرسالة مكونة من ٣٤٠٠ كلمة أو ١٠٠ كلمة مثلاً، فإن القيمة الاختبارية الناتجة عن معالجة هذه الرسالة تكون مجموعة ثابتة الطول من الحروف (١٠٠ حرف مثلاً)، والمهم أن هذه القيمة تكون غير متكررة أو أن احتمال تكررها إذا اختلف نص الرسالة أو حجمها هو احتمال ضئيل للغاية ولا يكاد يذكر، فكل رسالة تنتج عنها قيمة اختبارية مختلفة تمامًا.

٧ . ٥ . ٣ التوقيع الرقمي

التوقيع الرقمي هو المقابل الإلكتروني للتوقيع المعتاد في البريد العادي، وفائدة وجود التوقيع الرقمي ضمن الرسالة هو التأكد من شخصية المرسل، ويتم إنشاء التوقيع الرقمي عن طريق تشفير القيمة الاختبارية المستنتجة من الرسالة (يتم هذا التشفير باستخدام المفتاح السري للمرسل)، وهكذا يتكون لدينا التوقيع الرقمي الذي تتم إضافته بعد ذلك إلى الرسالة، ولا يكون التوقيع الرقمي قابلاً للتزييف لأنه يستخدم المفتاح السري للمرسل.

٧ . ٥ . ٤ تضافر التقنيات لتحقيق أمن البريد الإلكتروني

لما كانت القيمة الاختبارية مستخلصة من نص الرسالة، ولما كانت الرسالة المشفرة تضم التوقيع الرقمي، وتضم كذلك المفتاح العلني للطرف المرسل، فيصبح من الممكن عن طريق المزج بين استخدام القيمة الاختبارية والتشفير بواسطة المفاتيح العلنية تحقيق الأهداف الثلاثة لأمن البريد الإلكتروني وهي: التأكد من سلامة محتويات الرسالة، والتحقق من شخصية المرسل، وتوثيق الرسالة (ضمان عدم إنكار المرسل مسئوليته عنها)، ويتم ذلك على النحو التالي:

للتأكد من أن الرسالة قد وصلت صحيحة دون أن تتعرض للتعديل وللتحقق من شخصية مرسلها في الوقت نفسه يقوم الطرف المستقبل باستخدام نص الرسالة التي وصلته (قبل فك شفرتها) لتوليد القيمة الاختبارية منها، ثم يقوم بفك شفرة التوقيع الرقمي المصاحب للرسالة مستخدمًا في ذلك المفتاح العلني للمرسل فيستخلص بذلك القيمة الاختبارية من الرسالة، وبعد ذلك يقوم الطرف المستقبل بمقارنة القيمة الاختبارية المولدة بالقيمة الاختبارية المضمنة في رسالة المرسل فإذا تطابقتا فإن ذلك يؤكد أن محتويات الرسالة صحيحة ولم تتعرض للتعديل.

وحيث أن المفتاح السري للمرسل هو وحده الذي يمكنه تشفير القيمة الاختبارية للرسالة لتوليد التوقيع الرقمي فإن ذلك يؤكد شخصية الطرف المرسل (ربما ليس بشكل قاطع بافتراضأن أي شخص يمكنه الحصول على المفتاح السري للطرف المرسل يكون في مقدوره توليد التوقيع الرقمي).

أما الخصوصية فيمكن تحقيقها عن طريق استخدام الطرف المرسل للمفتاح العلني الخاص بالشخص الذي ينوي إرسال الرسالة إليه (الطرف المستقبل) عند قيامه بتشفير الرسالة نفسها، وبذلك لا يمكن فك شفرة هذه الرسالة إلا عن طريق المفتاح السري للطرف المستقبل.

٧ . ٥ . ٥ صندوق الشفرة المغلق (الغلاف الرقمي)

يتم حاليًا تحقيق هذا المزج بين التقنيات الثلاث السابق ذكرها عن طريق إنشاء ما يسمى «صندوق الشفرة المغلق»، أو «تقنية الأغلفة الرقمية» حيث يتم عشوائيًا توليد مفتاح شفرة سري من نوع (DES) (وهو «أسلوب تشفير البيانات المعياري») ويستخدم هذا المفتاح في تشفير الرسالة. هذا المفتاح السري يتم وضعه في «صندوق الشفرة المغلق» بعد تشفيره باستخدام المفتاح

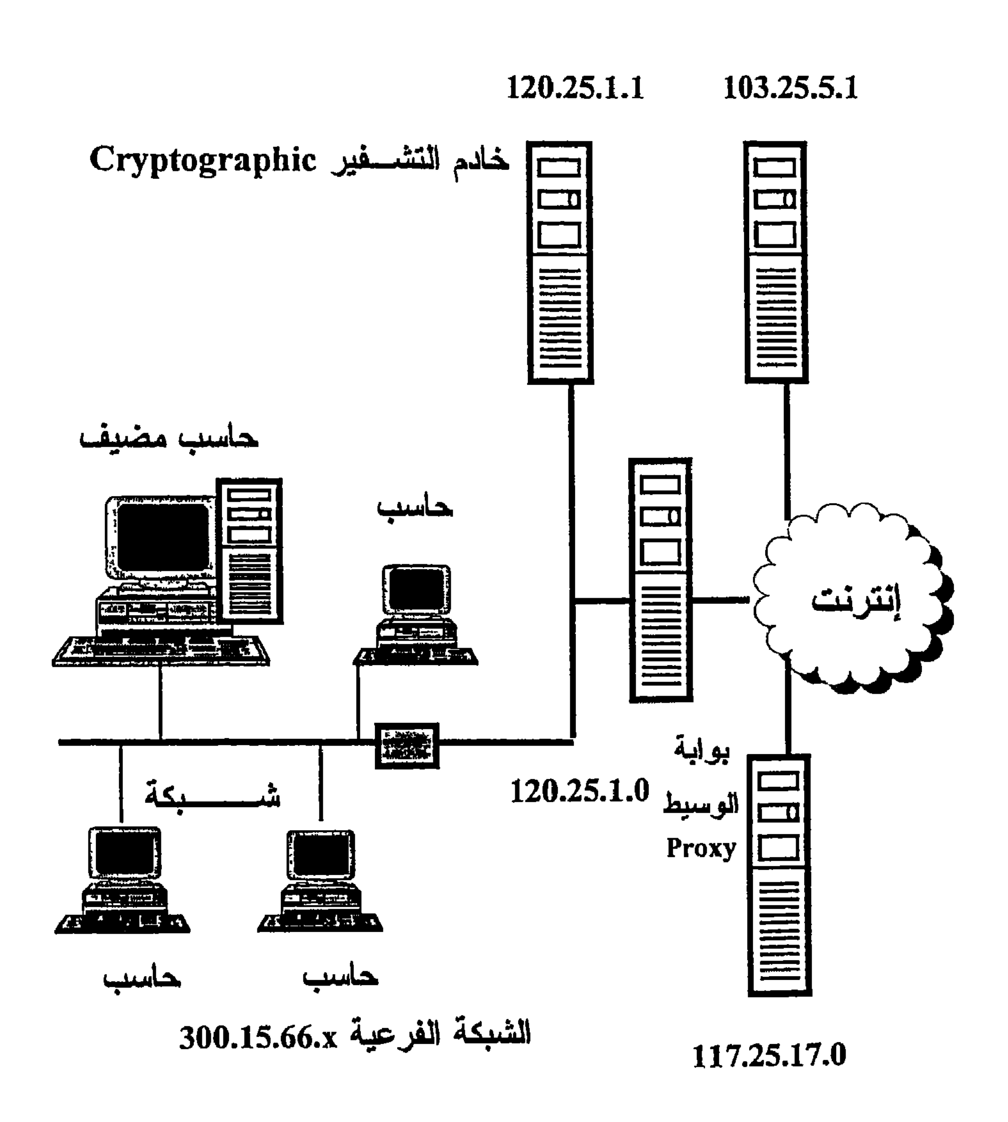
العلني، وهو من نوع (RSA) «رايفست وشامير وآدلمان» للطرف الذي سوف ترسل إليه الرسالة (الطرف المستقبل). أما توقيع الرسالة فيتم توليده كما ذكرنا سابقًا. ثم يتم إرسال الثلاثة معًا (توقيع الرسالة، والصندوق المغلق الذي يحتوي على المفتاح الذي استخدم في تشفير الرسالة، والرسالة المشفرة نفسها) إلى الطرف المستقبل. في هذه الحالة لا يستطيع أحد سوى الطرف المستقبل قراءة هذه الرسالة لأن المفتاح (DES) قد تم تشفيره باستخدام المفتاح العلني لهذا الطرف المستقبل دون غيره، وهكذا يقوم الطرف المستقبل باستخدام مفتاحه السري لفك شفرة المفتاح السري المستخدم في تشفير الرسالة، وبعد الحصول على المفتاح يمكنه (فتح) الصندوق المغلق أي فك شفرة الرسالة.

٧ . ٦ بوابة التشفير (Encryption Gateway)

إذا كانت لدينا منظمة لديها ثلاثة فروع في ثلاث مدن مختلفة يتم الربط بينها عن طريق شبكة الإنترنت، فعادة يوجد «جدار حماية» (Fire Wall) في نقطة اتصال كل فرع بالإنترنت لحمايته من الاختراق. ومن الطبيعي أن يكون هناك كم كبير من الاتصالات ينساب فيما بين الفروع الثلاثة حول شئون العمل بالإضافة إلى اتصال هذه الفروع مع مواقع أخرى. ولذلك فمن المنطقي أن تعمد المنظمة إلى تشفير كل البريد الإلكتروني المتبادل فيما بين هذه المواقع الثلاثة.

الحل في هذه الحالة يمكن أن يكون تركيب «محطة تشفير» (Cryptography Server) منفصلة بالإضافة إلى جدار الحماية. ويستخدم هذا الأسلوب، الذي يعتمد على الحماية بالتشفير، لإنشاء ما نطلق عليه «الشبكة الخاصة الافتراضية» (Virtual Private Network)، وهي الشبكة المغلقة من الناحية العملية. ولما كان البريد الإلكتروني يمر دائمًا من جدار

الحماية عن طريق منفذ ٥٢ (في حالة استخدام SMTP)، ولأن عناوين إنترنت للحاسبات المضيفة عادة ما تكون ثابتة، فيمكن تنفيذ هذا الحل بشكل مباشر كما يبين الشكل (٧ ـ ١).



شكل (٧ ـ ١) بوابة التشفير Cryptographic Gateway

يبين الشكل كيف يشترك الوسيط العادي مع حاسب آخر في الشبكة الداخلية نفسها، وهذا الحاسب يتولى تقديم خدمة تشفير تشبه ما يقدمه «نظام البريد عالي الخصوصية» (Privacy Enhanced Mail) أو (PEM). يقوم هذا الحاسب ولنطلق عليه «خادم التشفير» (Encryption Server) بعملية التشفير على أساس الحاسب المضيف وليس على أساس المستفيد كما يفعل نظام (PEM) القياسي، فالرسالة التي يريد المستفيد إرسالها إلى مستفيد آخر بموقع آخر بالشبكة (بالعنوان ١ . ٥ . ٢٥ . ١٠٣ مثلاً) يجب أن ترسل أولاً إلى «خادم التشفير» الذي يقوم بتشفير الرسالة باستخدام مفتاح معلوم لدى الموقع (١ . ٥ . ٢٥ . ١٠٣)، وهو موقع المرسل إليه. وعند إرسال أي رسالة يقوم جدار الحماية باختبار عنوان المصدر لهذه الرسالة فإذا كان العنوان هو أحد عناوين الشبكة الفرعية X . ٦٦ . ١٥ . ٣٠٠ فإن الرسالة يجب تشفيرها، وهنا تقوم بوابة الوسيط بتوجيه الرسالة إلى العنوان (١ . ١ . ٢٥ . ١٢٠)، وهو عنوان خادم التشفير، بينما الرسالة التي مصدرها العنوان (١ . ١ . ٢٥ . ١٢٠) فمن المفروض أنها مشفرة بالفعل لأنها آتية من خادم التشفير ومن ثم يجب توجيهها إلى وجهتها مباشرة (١ . ٥ . ٢٥ . ١٠٣)، وعندما تصل الرسالة إلى وجهتها النهائية يتم إزالة التشفير.

هذه العملية كان من الممكن أن تتم بواسطة جدار حماية واحد، ولكن ذلك كان من الممكن أن يزيد من احتمالات تعريض بيانات المنظمة للانتهاك إذ إن نجاح اختراق جدار الحماية قد يعرض مفاتيح التشفير نفسها للانكشاف، ولذلك فمن الأضمن تنفيذ التشفير على خادم تشفير مستقل، أو باستخدام أجهزة تشفير خاصة (أجهزة حاسب متخصصة لتشفير البيانات).

من المهم ملاحظة أن عملية التشفير وفك الشفرة ليس من الضروري أن تتم عن طريق المستفيد، فعادة لا يدري المستفيد إطلاقًا أن رسائله يتم

تشفيرها. وهذا التوجه ينجح في حماية المنظمة من محاولات انتهاك السرية أو تزوير البيانات مهما كانت أخطار الانتهاك المحدقة بالشبكة المتصلة بإنترنت وذلك بأقل تكلفة.

٧ . ٧ اختيار أسلوب حماية البريد الإلكتروني

كثير من مشاكل الأمن التي يتعرض لها البريد الإلكتروني يمكن حلها من خلال الاختيار الواعي للحلول الأمنية للشبكات والمتاحة في الأسواق ثم تطبيق هذه الحلول بعناية. وفيما يلي بعض الأخطار الأساسية التي يتعرض لها البريد الإلكتروني وكيفية مواجهتها:

٧ . ٧ . ١ التقاط المعلومات الحساسة بواسطة متلصصين

طالما أن البريد الإلكتروني الذي يتم نقله عبر الشبكات يكون في معظم الأحيان في صورة نصوص حرفية بسيطة فمن الممكن لأي شخص غير مرخص له، إذا ما استطاع استقباله، أن يطلع عليه أو أن يعدل من محتوياته أو أن يقوم بتزوير المعلومات الواردة فيه. وما دام هذا الاختراق، في معظم الأحوال، لا يمكن اكتشافه سواء بواسطة الطرف المرسل أو الطرف المستقبل فإنه كثيرًا ما يمر دون أن يلاحظه أحد.

وبينما ينطبق ذلك على كل من الشبكات المحلية والشبكات الكبيرة فإن شبكة إنترنت بالذات وكذلك الشبكات الداخلية للمؤسسات (إنترانت) هي المعرضة على وجه الخصوص لهذا النوع من الاختراقات الأمنية. وربما كان هذا هو الميدان المناسب لاستخدام التشفير و«التوقيعات الرقمية» وتحديد الشخصية لسد هذه الثغرة.

٧ . ٧ . ٢ إرسال الملفات

يرجع الفضل في انتشار البريد الإلكتروني في عالم المال والأعمال، وفيما وجده من قبول كبير في هذا الميدان، إلى قدرته على نقل الملفات المركبة (وليست ملفات النصوص البسيطة الخالية من الصياغة)، وتحتوي هذه الملفات على الرسوم البيانية وعلى الصور وغير ذلك من أشكال البيانات. وبالرغم من الفوائد الأكيدة لهذه الملفات فإن إلحاقها بالرسائل قد ينطوي على بعض المخاطر الحقيقية، فهي قد تحتوي على الفيروسات أو على بعض الملفات القابلة للتنفيذ (البرامج) والتي قد تكون ذات خطر بالغ على أمن الشبكة وسلامتها. ففي حين أن الضرر الذي قد تحدثه الفيروسات معروف مداه جيدًا إلا أن الملفات القابلة للتنفيذ والتي قد يتم إلحاقها برسائل البريد الإلكتروني يمكن أن ينتج عنها آثار أكثر ضررًا، فعلى سبيل المثال «حصان طروادة» هو برنامج يمكن استخدامه لإرسال هذه الملحقات غير البريئة. والأخطر من ذلك هو القدرة على استعادة هذه الملفات بشكل مستتر محملة ببعض المعلومات السرية (مثل كلمات السر) أو بعض المعلومات الحساسة للمؤسسة، وهذه تعتبر واحدة من أعظم الأخطار التي تهدد أمن المعلومات، فالمتسللون ومحاولو الاختراق، إذا ما كانوا مسلحين بكلمة سر، فإنهم بذلك يكون لديهم مفتاح خزائن المعلومات الموجودة على الشبكة. ولعلاج هذه المشكلة تستخدم بعض البرمجيات الأمنية البسيطة مثل «حائط النار» (Firewall).

٧ . ٧ . ٣ عدم حماية البريد الإلكتروني بعد تخزينه

بينما تولي معظم المؤسسات عناية فائقة لحماية البريد الإلكتروني المرسل منها أو المستقبل بواسطتها، إلا أنها لا تبدي نفس الاهتمام بالبريد بعد أن يتم تخزينه على وسائط التخزين فيها. وطالما أن البريد الإلكتروني

قليلاً ما يتم حذفه بعد استقباله فإن المعلومات الحساسة التي يتضمنها يتم تخزينها في ملفات، وهذه الملفات تكون عرضة للقراءة من جانب كل من له قدرة على استخدام جهاز الحاسب والوصول إلى هذه الملفات، ويفتح هذا الخطأ الباب واسعًا لإمكانية حدوث حوادث مؤسفة. ويمكن سد هذه الثغرة باستخدام وسائل عديدة ربما كان أفضلها استخدام أجهزة «توزيع خدمة» (Servers) مؤمنة جيدًا لاستقبال وتخزين البريد الإلكتروني في المؤسسات.

ونود هنا أن ننبه إلى ضرورة اهتمام المؤسسات والأفراد بأمن الاتصالات بصفة عامة والبريد الإلكتروني بصفة خاصة، وضرورة أخذ معايير الأمن المذكورة سابقًا بعين الاعتبار عند اقتناء نظم البريد الإلكتروني. كما نود أن نؤكد على أن عملية التأمين لا تكون ناجحة إلا إذا شملت كلاً من تأمين الشبكة وتأمين الرسالة معًا أخذًا بمفهوم الأمن الشامل.

الفصل الثامن

تداول النقود الإلكترونية

٨ . ١ النقود الإلكترونية.

٨ . ٢ حماية النقود المتداولة عبر الإنترنت.

٨ . ٣ الكتاب الذي كلف صاحبه الكثير.

٨ . ٤ الأسهم والسندات إلكترونياً.

٨ . ٥ نظام الدفع الآلي على الإنترنت.

٨ . ٦ التسوق الآمن عبر الإنترنت.

٨ . ٧ مستقبل جرائم المعلومات في مجال الأعمال.

تداول النقود الإلكترونية

يتعرض هذا الفصل لما اصطلح على أنه «نقود إلكترونية» وهي تلك النقود التي يتم تداولها من خلال أجهزة الحاسب وشبكاته. فنبدأ بالحديث عن هذا النوع من النقود، ثم نتحدث عن الجهود الحالية لحماية النقود المتداولة عبر الإنترنت، ثم نورد مثالاً عن حادثة سرقة من خلال سرقة رقم بطاقة الدفع الآلي لأحد الأفراد. ونتحدث بعد ذلك عن إمكان تحويل الأسهم والسندات لتصبح إلكترونية هي أيضًا! ، ونتحدث عن نظام للدفع الآلي في هونج كونج. ثم نقدم مجموعة من النصائح المهمة التي تضمن تسوقًا آمنًا (إلى حد كبير) عبر شبكة الإنترنت. ونختتم هذا الفصل بمحاولة تصور مستقبل جرائم المعلومات في مجال الأعمال وأحجام الخسائر المنتظرة في هذا المجال مستقبلاً.

٨ . ١ النقود الإلكترونية

يقول «جاك وذرفورد» الباحث في تاريخ البشرية في كتابه الممتع «تاريخ النقود» (Weatherfor,1997) أننا نعيش الآن بداية الثورة النقدية الثالثة، إذ حدثت الأولى منذ نحو ٢٥٠٠ سنة عندما بدأ البشر في استخدام العملات المعدنية بدلاً من الأصداف! أما الثورة النقدية الثانية فقد جاءت في القرن الخامس عشر مع ظهور النقود الورقية. أما الثالثة فقد استخدمت البشرية فيها النقود الإلكترونية (e - cash) أو (cyber cash)، ويتنبأ «وذرفورد» بأن النقود الإلكترونية سوف تكون مكملة (لا بديلة) للعملات المعدنية والورقية (وحتى البلاستيكية التي تمثلها حاليًا بطاقات الائتمان). وربما كان السبب في ذلك هو وجود كم هائل من هذه العملات يتم تداوله بالفعل بين الناس

(وسيظل كذلك) برغم تزايد الاعتماد على بطاقات الائتمان والنقود الإلكترونية، ولكن الثقة المتنامية في المعلومات الإلكترونية (حيث يثق كثير من الناس بكل ما هو معروض على الإنترنت) سوف تؤدي في النهاية إلى ثقة متنامية في تداول النقود الإلكترونية.

وربما سوف نحتاج في القريب العاجل إلى مكان مثل «الجنادرية» لرؤية الصرافين التقليديين والبنوك والنقود الورقية (نقود ذلك الزمان البعيد!!)، وربما أدى ذلك إلى اختراع وسائل أكثر أمنًا لتداول هذا النوع من النقود. ولكن للأسف من المتوقع أن يحدث المزيد من الجرائم والمزيد من الخسائر الجسيمة قبل أن نصل إلى هذه الوسائل الأكثر أمنًا والتي لابد أن تكون شاملة مانعة، أي أن تكون الشبكة آمنة، والحاسب آمنًا، ووسائل الإدخال والإخراج آمنة . . . وهكذا. فالأمن لا يتجزأ، ونشبه الأمن بالقربة (وعاء الماء الجلدي القديم) حيث يؤدي أي ثقب فيه إلى تسرب الماء كله!.

٨ . ٢ حماية النقود المتداولة عبر الإنترنت

بعض المعلومات تكون لها قيمة النقود، ولذلك تحتاج هذه المعلومات إلى درجة أكبر من الأمن. مثال ذلك قيمة المبلغ المطلوب تحويله من حساب إلى آخر في البنك، أو المبالغ التي يتم خصمها من حساب البطاقة الائتمانية لينتقل المبلغ من رصيد صاحب البطاقة في ا لبنك إلى رصيد الشركة التي تعامل معها. والكمبيوتر في كل من البنكين يختزن هذه المعلومات وينفذ هذه العمليات. ويقترح «د. بوب بلاكلي» (Blackley,1997) وسائل ربما اعتبرناها غير عملية لحماية المعلومات التي تحمل قيمة مالية. فيقول «بوب بلاكلي» أن مبلغ مليار دولار من فئة المائة دولار الورقية يحتل حيزًا حجمه حوالي ١٥ ياردة مكعبة، وقيمة هذا المبلغ مقومة بالذهب تزن حوالي ٨٠

طنًا من الذهب، بينما قيمة هذا المبلغ إلكترونيًا، أو ما يسمى «بالنقد الإلكتروني» (Electronic Cash)، فهي لا تحتل حيزًا أكبر من ٣٢ رقم ثنائي (bit) بالإضافة إلى بعض ا لبيانات الإضافية التي يتم تمثيلها بواسطة عدد محدود من الحروف. ويقول «بلاكلي» إن هذه دعوة صريحة للتزوير، ويقترح أنه إذا كنا نرغب في تأمين النقد الإلكتروني فلابد أن نبدأ بإعطائه حجمًا أو حيزًا ماديًا يتناسب طرديًا مع قيمته.

أوقفت بريطانيا استخدام نظام «المفتاح الاختباري القياسي» (Standard Test Key) أو (STK) الذي درجت البنوك البريطانية على استخدامه منذ عام ٠٨٩١ للتحقق من صحة الرسائل الخاصة بالتحويلات المصرفية بين البنوك بحيث يستبدل بكل معلومة (مثل اسم البنك أو التاريخ أو قيمة المبلغ المحول) رمز رقمي مأخوذ من كتاب خاص بالرموز. ويقوم الكمبيوتر الخاص بالبنك بجمع هذه الأرقام للحصول على رقم يسمى «المفتاح الاختباري» والذي يتم تسجيله في نهاية الرسالة، وبذلك يمكن اكتشاف أي خطأ أو تعديل يمكن أن يطرأ على الرسالة بعد إرسالها من البنك المرسل، إذ أن قيمة المفتاح الاختباري سوف تختلف في هذه الحالة. ولكن ثبت عدم فاعلية هذا النظام حيث أنه لا يمكن من خلاله اكتشاف تغيير مكان بعض الأرقام، فالمبلغ ٢١٣ , ٩٧٨ جنيهًا ينتج نفس الرقم الاختباري الذي ينتج إذا كان المبلغ هو ٩٧٨ , ٢١٣ جنيهًا مما يفتح للتزوير بابًا واسعًا.

٨ . ٣ الكتاب الذي كلف صاحبه الكثير

«دون جارلوك» هو باحث متخصص في مجال الإنترنت كان يشارك الشرطة في عملية تهدف إلى وقف جرائم الإنترنت ضد الأطفال. وعندما اكتشف فجأة في بداية شهر يونيو ١٩٩٩ أن رصيده في البنك قد وصل إلى

الصفر كان آخر سبب توقعه لذلك هو أن البحث عن الفاعل سوف يقوده إلى أخطر العصابات على شبكة الإنترنت. وقد استخدم «جارلوك» مهاراته في التقصي من خلال الإنترنت لحل مشكلته وكان طرف الخيط من شركة توريد الكتب العملاقة «أمازون» (Amazon.com) وقاده تتبع الخيط إلى عصابة من لصوص الإنترنت في بانجكوك بتايلاند. وكان «جارلوك» طوال فترة البحث يتعلم دروسًا غاية في الأهمية عن مخاطر التسوق الإلكتروني حتى في مواقع تدعي أنها «آمنة مائة بالمائة» (Masland,1999).

ووفقًا لمصادر البنك الخاص بالسيد «جارلوك» وهو بنك «مين ستريت» فقد قام شخص ما بشراء بضائع قيمتها ١٤٠٠ دولار من شركة «أمازون» من موقعها على الإنترنت (Amazon.com) وقيد هذه المشتريات على حساب بطاقة الائتمان الخاصة بجارلوك. عندما اكتشف جارلوك هذه الحقيقة شك في وجود عملية احتيال من نوع ما، فقد كان جارلوك عميلاً قديمًا أمضى سنوات عدة في التعامل مع هذه الشركة، وكانت كل تعاملاته متواضعة لا تتجاوز ١٦٠ دولارًا، فاتصل بالشركة ليعرف من المسئول عن ذلك. ولدهشته الشديدة فقد رفضت الشركة الكشف له عن أية معلومات تخص حسابه أو إفشاء اسم الشخص الذي اشترى هذه البضائع مستخدمًا بطاقة جارلوك الائتمانية. بل رفضت الشركة أن تخبره عن نوعية البضائع التي تم شراؤها، أو العنوان الذي تم شحنها إليه. وتعللت الشركة بأن سياستها هي عدم الإفضاء بالمعلومات التفصيلية عن الحسابات إلا للبنك الخاص بالعميل فقط، حفاظًا على الخصوصية الفردية للعملاء! وكان كل ما حصل عليه جارلوك من معلومات هو (زلة لسان) من ممثل قسم خدمات العملاء عبر الهاتف حيث تلفظ عن غير قصد بالنصف الأول من عنوان البريد الإلكتروني للشخص الذي قام بالشراء، ثم توقف الموظف واعتذر عن عدم إمكان الإفضاء بالمعلومات.

صمم جارلوك أن يتولى البحث بنفسه فاكتشف مجموعة من الأدلة التي قادته إلى عصابة من محترفي الاحتيال باستخدام الحاسب الآلي مقرها بانجكوك في تايلاند، حيث كان النصف الأول من عنوان البريد الإلكتروني الذي حصل عليه هو أحد الأسماء الأولى الشائعة الاستخدام في تايلاند. واستطاع بمعاونة أدوات البحث على الإنترنت (Search Engines) الكشف عن أسماء وعناوين الأفراد الذين استخدموا بطاقته وأرقام هواتفهم وجهات عملهم، وكان معظمهم من الطلبة الجامعيين.

في نهاية الأمر كشفت شركة «أمازون» عن العنوان الذي تم شحن البضائع إليه وعنوان البريد الإلكتروني الذي استخدمه اللصوص لإتمام عملية الاحتيال. وتم تحويل القضية إلى الشرطة الدولية (الإنتربول) حيث كشفت تحقيقاته أن هذه العصابة قامت من قبل بعدة سرقات من نفس الشركة باستخدام أرقام بطاقات ائتمان مسروقة. وأعلنت الشركة أنها سوف ترد أية مبالغ يتم اقتطاعها من رصيد العميل بطريق الاحتيال ما لم يقم البنك برد هذه المبالغ.

ربما ما جعل مشكلة جارلوك أكثر صعوبة هو أن الذي تم كشفه في هذه الحالة كان رقم «بطاقة الدفع» الخاصة به (Debit card) وليس «بطاقة الائتمان» (Credit Card)، فلو كانت المشكلة مع بطاقة الائتمان لكان من السهل عليه أن يمتنع عن الدفع وتنحصر مسئوليته في مبلغ ٥٠ دولارًا فقط لا أكثر، ولكن لأن بطاقة الدفع هي التي فقدت فقد تم سحب رصيده كله بمجرد شحن البضاعة.

الآن يثور السؤال الهام وهو كيف عرف الجناة رقم بطاقة جارلوك؟ هل عرفوه من موقع شركة «أمازون» أم عرفوه عن طريق آخر؟ أم أنهم قاموا بتوليده بشكل عشوائي؟ والإجابة عن هذا السؤال تهمنا كثيرًا. نفى المتحدث باسم الشركة بشكل قاطع أن يكون الجناة قد حصلوا على الرقم من موقع

الشركة. ومن المعروف أنه من السهل على الجناة أن يحصلوا على البرنامج الذي تستخدمه البنوك لتوليد أرقام بطاقاتها، وبالتالي يمكنهم توليد أرقام عشوائية يقومون بتجربتها للتأكد من أنها أرقام موجودة بالفعل، وأن تاريخ صلاحيتها ما زال ساريًا، وأن هناك رصيد كاف لها يمكن الاستفادة منه.

ولكن كان على الشركة أن تنتبه إلى التناقض الحادث هنا، إذ أن البطاقة المستخدمة صادرة من الولايات المتحدة، بينما البضاعة مطلوب شحنها إلى تايلاند. فهذا الأمر لابد أن يلفت انتباه المسئولين في الشركة. وعن هذه النقطة تجيب الشركة أن اللص لم يستخدم حساب «جارلوك» لدى الشركة وإنما أنشأ حسابًا آخر مستقلاً باستخدام هذه البطاقة.

والآن لنتأمل الأمر بهدوء قبل أن نكيل الاتهام لشبكة الإنترنت والتجارة الإلكترونية والتقنية بصفة عامة.. أيهما أكثر أمنًا: أن تدخل رقم بطاقة الائتمان على الإنترنت أم أن تعطي البطاقة للعامل في المطعم ليغيب فترة بالداخل ثم يعود إليك بالإيصال لتوقعه؟.. ما أدراك أن هذا العامل لم ينقل رقم البطاقة ويحتفظ به للاستخدام لاحقًا؟ وما أدراك أنه لم يستخدمه في طباعة عدة إيصالات يستخدمها فيما بعد خاصة أن صورة توقيعك موجودة لديه؟ أي أن التسوق الإلكتروني برغم خطورته إلا أنه لا يزيد خطورة عن التسوق غير الإلكتروني.

٨ . ٤ الأسهم والسندات إلكترونياً

اندلعت في الولايات المتحدة الأمريكية معركة سياسية كبرى خلال حقبة الثمانينيات من القرن العشرين عندما قُدم للكونجرس اقتراح بتحويل صكوك ملكية الأسهم والسندات إلى الصورة الإلكترونية، أي أن تصبح مجرد سجل إلكتروني في ملف مخزن على الحاسب. وثار المستثمرون

الذين كانوا يريدون الاحتفاظ بصكوكهم في أيديهم غير مؤمنين بفكرة أن تتحول صكوكهم إلى مجرد بيان مخزن في أحد حاسبات شركة السمسرة، فكيف للمستثمر أن يتأكد من أن خطأ ما لن يتسبب في محو بيانات صكوكه من الحاسب؟ ومن أين له أن يثق في أن صلاحية وسائط التخزين يمكن أن تمتد عشرات السنين؟ وهم في هذه النقطة بالذات على حق إلى حد ما، فالبيانات المخزنة مغناطيسيًا على الأقراص أو الأشرطة المغنطة تزول بعد فترة من الزمن، ولذلك نقوم باستمرار بتحديثها وإعادة كتابتها على وسط آخر. ونظرًا لكثرة المستجدات في مجال التقنية فأنى للمستثمر أن يتأكد من أن أجهزة قراءة الأشرطة أو الأقراص التي خزنت بياناته عليها ستظل موجودة بعد عشرات السنين؟ فربما تبقى الأشرطة والأقراص ولكن تختفي الأجهزة القادرة على قراءتها وتظهر أجهزة جديدة. وهذا التفكير ليس بغريب، فمن الصعب الآن أن نجد أجهزة تقرأ الأشرطة المستديرة (Reel tapes) بعد أن تحولت معظم مراكز الحاسب الآلي إلى الأشرطة المربعة (Cartridges).

هذا في الولايات المتحدة حيث حسمت المعركة في عام ١٩٩٠ لصالح الصكوك الورقية بقرار من الكونجرس الأمريكي، بينما في فرنسا والعديد من دول الاتحاد الأوروبي فالصورة مختلفة، إذ تحولت الصكوك فيها إلى سجلات إلكترونية بالفعل.

٨ . ٥ نظام الدفع الآلي على الإنترنت

تم الاتفاق بين أكبر مؤسسة مصرفية في «هونج كونج»، وهي مؤسسة «هونج كونج وشنغهاي البنكية» (HSBC)، وشركة «كومباك» لأجهزة الحاسب على تطوير أول نظام آلي آمن للتجارة الإلكترونية. واعتبارًا من شهر أكتوبر ١٩٩٩ فإن هذه الخدمة تمنح التجار نظام دفع (آمن) لقبول

المدفوعات عبر شبكة الإنترنت بواسطة البطاقات الائتمانية (HongKong,1999) . وقد وفرت شركة «كومباك» البنية التحتية اللازمة لإتمام عمليات الدفع من العملاء للشركات وبين الشرات وبعضها البعض . ويتضمن هذا النظام الآليات الأمنية الكفيلة بتأمين العمليات الإلكترونية . وقد دفع إلى هذه الخطوة، التي سبقتها خطوات مماثلة في أوروبا والولايات المتحدة واليابان، الرغبة الهائلة المتولدة لدى جمهور المتعاملين مع الشركات لإنهاء معاملاتهم بالكامل من خلال شبكة الإنترنت . وكانت العقبة الوحيدة التي تحول دون القفزة الكبيرة للتجارة الإلكترونية هو أمن المعاملات على الشبكة، ولكن آليات التشفير القوية المستخدمة في هذا النظام وغيره من النظم التي تستخدم «أجهزة الخدمة الآمنة» (Secured Servers) كسرت، إلى حد ما، حاجز الخوف الذي كان يجعلنا نحجم عن ذكر بيانات بطاقاتنا الائتمانية على الشبكة . وساهم في ذلك دخول البنوك كطرف ثالث بين الشركة البائعة وبين العملاء مما يطمئن العميل إلى أن البنك يضمن له حقوقه فيما لو أسيء استخدامها .

٨ . ٦ التسوق الآمن عبر الإنترنت

هناك بعض الملاحظات التي يجب مراعاتها عند التسوق الإلكتروني :

- تحقق من موقف الشركة التي تنوي الشراء منها وذلك من خلال استفسارك عنها من موقع : (Better Business Bureau) .
- إذا لم تكن سمعت بهذه الشركة من قبل فاطلب الكتالوج الخاص بها أو معلومات عنها بالبريد قبل التعامل معها .
- اهتم بالمحافظة على سرية كلمة المرور الخاصة بك على جميع المواقع .
- استخدم في الدفع دائمًا بطاقة الائتمان (Credit Card) وليس بطاقة الدفع (Debit Card) .

- اطبع باستمرار نسخة من أمر الشراء الخاص بك ورقم رسالة التأكيد الذي ترسلها لك الشركة.
- إذا لاحظت أن الشركة تسألك عن معلومات غريبة مثل رقم الهوية أو رقم الإقامة أو رقم الضمان الاجتماعي فعليك أن تتحرى عن السبب.
- تأكد من أن الشركة لديها رقم هاتف.
- تأكد من خلال دليل الهاتف أن الرقم المذكور هو بالفعل مسجل باسم هذه الشركة.

٨ . ٧ مستقبل جرائم المعلومات في مجال الأعمال

من الواضح بصفة عامة أن حجم الخسارة في العملية الواحدة من جرائم المعلومات في مجال الأعمال في ازدياد مستمر، بينما عدد الجرائم من هذا النوع بالنسبة للحجم الضخم من العمليات المالية التي تتم كل يوم هو في تناقص مستمر (Parker,1998). والمتوقع أن يتناقص عدد جرائم المعلومات خلال العقد الأول من القرن الحادي والعشرين بسبب الاتجاه السائد حاليًا نحو استخدام المزيد من الضوابط وزيادة فاعلية هذه الضوابط في حماية الحاسبات وشبكات الاتصال، وكذلك انتباه المؤسسات لأهمية تسجيل كافة الوقائع مثل دخول الأفراد إلى النظام واستخدامهم للمعلومات المخزنة في الحاسب، بالإضافة إلى ازدياد الاهتمام بالتحليل الآلي لهذه الوقائع لتسليط الضوء على الوقائع المشبوهة مما يسهل على مسئولي أمن المعلومات اكتشاف الجريمة فور وقوعها أو ربما قبل وقوعها (خلال المحاولات التمهيدية التي تسبق ارتكاب الجريمة)، فيمكن مثلاً اكتشاف تكرار تنفيذ عملية إضافة أو خصم من الرصيد مرتين، بل يتم هذا الاكتشاف قبل أن يتم صرف المبلغ من الحساب المستفيد أو تحويل المبلغ إلى البنك الآخر.

هناك سبب آخر وجيه وراء الاعتقاد بأن جرائم نظم المعلومات سوف يتناقص عددها في العقد القادم. هذا السبب هو انتشار استخدام التشفير، وهي الوسيلة التي يمكن أن تؤثر بشكل هائل في تقليص، أو ربما في منع، هذا النوع من الجرائم خاصة عمليات التنصت أو الاختراق أو تزوير العمليات المالية. ولكن من المهم أن نعلم أن استخدام التشفير وحده لن يقضي على هذه الجريمة تمامًا، فالبرامج عليها في النهاية أن تفك شفرة المعلومات قبل عرضها على المستفيد، وهنا مربط الفرس، فالبشر ربما كانوا أضعف الحلقات في منظومة أمن المعلومات. فالتشفير في الواقع لا يفعل سوى أنه ينقل مكمن الخطر من الشبكات والحاسبات إلى البشر، وبذلك يجب أن تكون هناك ضوابط مصاحبة للتشفير لاكتمال الفائدة.

ولكن علينا أن ننتبه إلى أن التقدم التقني الذي يساعد على مكافحة الجرائم إنما يقوم في الوقت نفسه بمساعدة المجرمين الذين يزدادون خبرة واستخدامًا للتقنية يومًا بعد يوم مما يجعلنا نتوقع ازدياد حجم الخسارة الذي يتحقق في الجريمة الواحدة مع ازدياد حجم استخدام التجارة الإلكترونية الذي يأخذ منحنى تصاعديًا. فعلينا أن نضع في الاعتبار أن مجرم الغد لن يخاطر باحتمال انكشاف أمره بعد تخطي الحواجز الأمنية العديدة من أجل مبالغ ضئيلة، ولكنه سوف يجري وراء الصيد السمين. وليس بعيدًا عن الذاكرة واقعة التزوير التي تعرض لها بنك «بارينجز» وكان حجم الخسارة فيها ٨٦٩ مليون جنيه إسترليني أي حوالي مليار ونصف من الدولارات الأمريكية والتي ما زالت أصداؤها تدوي في عالم المال والأعمال.

وليس بعيدًا ما حدث في عام ١٩٩٦ من محاولة الاحتيال التي وقعت في روسيا لتحويل عشرة ملايين دولار إلى مصارف مختلفة موزعة على أنحاء العالم، وكذلك قضية شركة التأمين على الاستثمارات (EFI) التي

سوف نتعرض لها في هذا الفصل والتي بلغ حجم الخسارة فيها بليونا دولار. وربما لولا استخدام الكمبيوتر في هذه الجرائم لانخفض حجم الخسائر عن ذلك بشكل كبير، ولعلنا نعلم جميعًا كيف أن نقل الفاصلة العشرية من مكانها رقمًا واحدًا يمكن أن يؤدي إلى خسائر ضخمة.

والمجرم هنا عليه أن يختار، فإذا قرر أن يكون حجم العملية كبيرًا فستكون النتيجة أن الضحية لن يكون أمامه سوى ملاحقة المجرم مهما كلفه ذلك. وإذا قرر أن يكون حجم العملية صغيرًا فالمبلغ المختلس لن يكون كافيًا للهروب من البلاد أو للصرف على القضية إذا تم ضبطه.

ويكشف «بوب كورتني» الخبير في أمن الحاسبات قضية المندوب المالي الذي اختلس عدة ملايين من الدولارات، الأمر الذي سبب بالغ الحرج لإدارة الشركة الكبيرة التي ينتمي إليها هذا المندوب والتي تحتل مكانها المرموق في شارع المال «وول ستريت». كانت هذه الشركة تعتبر من أكثر الشركات خبرة في إدارة الأموال، فما كان منهم إلا أن دعوا هذا المندوب المختلس إلى غداء عمل، وخلال جلسة طويلة تم الاتفاق معه على أن يدعوه يحتفظ بما حصل عليه من أموال في مقابل أن يعدهم بمغادرة المدينة فورًا وبصفة نهائية وأن يكتم هذه القصة في صدره إلى الأبد.

الفصل التاسع
الفيروسات

٩ . ١ الفيروسات وجريمة نظم المعلومات .

٩ . ٢ أنواع الفيروسات .

٩ . ٣ مقاضاة صانعي الفيروسات .

٩ . ٤ الإنذار الكاذب عن الفيروسات .

٩ . ٥ الفيروس من الناحية الجنائية .

الفيروسات

خصصنا هذا الفصل لمناقشة قضية الفيروسات لخطورتها الشديدة، فكتابة الفيروس هي في حد ذاتها من أخطر جرائم نظم المعلومات، ونشره في حاسبات الآخرين هو جريمة أخرى لا تقل شرًا وخطورة. ثم نتحدث عن بعض أنواع الفيروسات مثل حصان طروادة، والقنابل المنطقية، وباب المصيدة، والفيروس المشفر، والفيروس متعدد الأشكال. ننتقل بعد ذلك إلى مناقشة مسألة مقاضاة صانعي الفيروسات وهل ذلك ممكن؟ ثم نتحدث عما نشهده من آن لآخر من إنذارات كاذبة عن الفيروسات. ونختتم الفصل بالحديث عن الفيروس من الناحية الجنائية.

٩ . ١ الفيروسات وجريمة نظم المعلومات.

يعرف الفيروس بأنه أي برنامج (أو مجموعة من التعليمات) التي تلحق ضررًا بنظام المعلومات أو بالبيانات، على أن تكون لديه القدرة على التضاعف والانتشار بأن يقوم عند تشغيله بزرع نسخ منه في البرامج المصابة. وتقوم الفيروسات في العادة بتحويل برامج الحاسب إلى ما نسميه «حصان طروادة» (Trojan Horse)، ويمكن أن تكون أحيانًا في شكل «القنابل المنطقية» (Logic Bombs) أو «باب المصيدة» (Trapdoor).

يقوم الفيروس عند دخوله إلى البرنامج المصاب بتغيير بعض التعليمات فيه مما ينقل التحكم في البرنامج إلى الفيروس، الذي يكون مخزنًا في مكان آخر من الذاكرة، فيقوم بما هو مطلوب منه ثم يعيد التحكم بعد انتهاء مهمته إلى البرنامج المصاب دون أن يترك وراءه أثرًا يدل عليه.

وتقوم بعض الفيروسات المتقدمة بإضافة مجموعة من التعليمات إلى

نظام التشغيل في الكمبيوتر المصاب، بحيث تجعل هذه التعليمات نظام التشغيل يتولى بنفسه نشر الفيروس في جميع البرامج الموجودة على الجهاز.

وقد تكون مهمة الفيروس هي تدمير البيانات الموجودة في الذاكرة أو مسح الملفات من القرص الصلب أو إدخال بعض التعديلات على البيانات.

ويوجد الآن أكثر من عشرة آلاف نوع من الفيروسات المعروفة التي تصيب الحاسبات الشخصية (Parker,1998)، بالإضافة إلى مجموعة أقل بكثير من الفيروسات المعروفة التي تصيب نظم التشغيل مثل «يونيكس».

أما فيما يخص الحاسبات المركزية (Main Frames)، فبرغم أن كتابة الفيروسات لهذه الحاسبات أمر ممكن إلا أنه لا توجد هناك فيروسات معروفة تصيب هذا النوع من الحاسبات، ربما كان ذلك لسهولة وصول صانعي الفيروسات للحاسبات الشخصية، وسهولة تداول هذه الحاسبات للبرامج الملوثة.

وصلت فيروسات الحاسب لمرحلة الجريمة وأصبحت إحدى جرائم نظم المعلومات في عام ١٩٨٧ عندما نشرت مجلة «نيوزداي» مقالاً كتبه «لو دولينار»، الصحفي المتخصص في جرائم الحاسب، والذي تحدث فيه عن ثلاثة فيروسات ظهرت خلال فترة شهرين، واستجابت بعض شركات البرمجيات لهذا الإنذار بإنتاج بعض برامج الحماية من الفيروسات، وربما كان هذا ما استثار صانعي الفيروسات وجعلهم يدخلون في لعبة من أشرس الألعاب التي عرفتها البشرية. فقاموا بإنتاج فيروسات أكثر ضراوة وأوسع انتشارًا لتقابلها شركات البرمجيات ببرامج أكثر ذكاء وأكثر قدرة وكفاءة على اصطياد هذه الفيروسات وإبطال مفعولها وإزالة آثارها.

واليوم ازدادت حدة هذه المعركة الشرسة بظهور أنواع جديدة من الفيروسات المشفرة والمتعددة الأنشطة. ومما زاد من حدة المشكلة أن الأدوات والمعارف اللازمة لكتابة برامج الفيروسات أصبحت متاحة على شبكة الإنترنت لتساعد كل من لديه النية على إعداد هذه الفيروسات وتمده بكل ما يحتاج إليه لينتج فيروسات أشد ضراوة وأحد ذكاء وأكثر إيذاء!.

برغم أن الفيروسات لا يمكن أن تنشط من خلال ملفات البيانات لأن هذه الملفات لا يمكن تنفيذها كبرامج، إلا أن الفيروسات تتغلب على ذلك بأن تأتي في صورة برامج صغيرة «ماكرو» يتم إلصاقها بملفات البيانات (الوثائق مثلاً). وبالتالي فعندما يقوم المستفيد بتشغيل برنامج معالجة كلمات مثل «وورد» لفتح وثيقة ما لقراءتها يتم تشغيل هذا «الماكرو» الملوث الملتصق بالوثيقة آليًا، وبذلك يتمكن الفيروس من العمل. ومن أمثلة هذا النوع من الفيروسات فيروس (Impostor)، وفيروس (Wazzu)، وفيروس «الكلب المجنون» (Maddog). ويقوم هذا الأخير بتغيير حرف (a) إلى (e) في كامل الوثيقة التي يصيبها، وهو يفعل ذلك فقط إذا صادف وقت تشغيل الوثيقة الساعة الثامنة مساء من أي يوم!.

٩ . ٢ أنواع الفيروسات

٩ . ٢ . ١ حصان طروادة

يعمل فيروس «حصان طروادة» عن طريق إقحام تعليمات دخيلة خلسة ضمن برامج الآخرين. وتنتشر فيروسات الحاسب في البرامج الأخرى والحاسبات الأخرى عندما يقوم الضحية بتشغيل بعض برامجه المصابة، فيتم عندئذ تشغيل الفيروس وانتقاله إلى مكان آخر. ويستفيد الفيروس من صلاحيات البرنامج الذي يحتويه.

ويستخدم المجرمون «حصان طروادة» لارتكاب عمليات النصب والاحتيال والاختلاس وسرقة الخدمات والتجسس والتخريب.

تعمد بعض المواقع على شبكة الإنترنت إلى إدخال بعض البرامج الصغيرة (Magic Cookies) في الملف الخاص بهذا النوع من البرامج (Cookies file) الخاص بالجهاز الذي يزور هذه المواقع من خلال شبكة إنترنت. هذا الملف (Cookies file) يحتفظ بمعلومات عن المستفيد صاحب الجهاز واختيارات العرض الخاصة به والتي تحدد كيف يفضل هذا المستفيد عرض المواد على الشاشة. هذا الملف يمكن أن يكون مفيدًا لكل من الموقع والمستفيد نفسه، ولكنه يمكن كذلك أن يشكل «حصان طروادة» مناسب للمقتحم حيث يمكن من خلاله إدخال التعليمات الملوثة التي تسبب الضرر للكمبيوتر.

ومن المهم أن نتذكر أنه عند زيارتك لأحد المواقع فإن هذا الموقع بدوره (يزور) حاسبك الشخصي، ولهذا السبب يجب تجنب المواقع المشبوهة تمامًا كما تتجنب الذهاب إلى الأماكن المشبوهة في أي مدينة تزورها. ومن الحكمة أن تحذف هذه الملفات (Cookies) قبل أن تستخدمها بعض هذه المواقع ضدك.

بالرغم من أنه من النادر أن نرى «حصان طروادة» مخصصًا للأجهزة (Hardware) إلا أن هذا النوع موجود، ويمكن أن يكون مصدر خطر على أمن الحاسب. ويطلق مصطلح «صنع الرقائق» (Chipping) على عملية صنع حصان طروادة خاص بالأجهزة، وتتضمن هذه العملية إدخال دوائر سرية بشكل مباشر إلى الرقائق خلال مرحلة التصميم أو التصنيع. والمقتحم الشهير «كيفن متنيك» كان، قبل القبض عليه بتهمة أخرى، يحاول إدخال بعض البيانات عن بعد في ملف المواصفات الخاص بتصميم بعض الرقائق الخاصة بحاسب «موتورولا».

٩ . ٢ . ٢ القنابل المنطقية

القنبلة المنطقية هي مجموعة من تعليمات الكمبيوتر التي تنفذ عملاً مؤذيًا عند توفر شروط معينة، هذه الشروط قد تكون مثلاً حلول ساعة معينة في اليوم، أو حلول يوم معين في السنة. ومازلنا نذكر الحادثة التي وقعت منذ سنوات في إحدى الدول العربية عندما قام أحد المبرمجين بوضع هذه المجموعة من التعليمات ضمن برامج الحاسب الخاصة بالشركة التي يعمل بها بحيث يتم محو جميع ملفات الشركة عندما يتم حذف اسمه من ملف المرتبات!.

٩ . ٢ . ٣ باب المصيدة

الفيروسات من نوع «باب المصيدة» (Trapdoor) هي سلسلة من التعليمات المتروكة سهوًا داخل البرامج أو التي يتم إقحامها عمدًا فيها ويستفيد منها المبرمج الشرير.

وفي أحد الأمثلة قام واحد من المبرمجين بإعداد برنامج الرواتب على نحو يسهل له إجراء اختبارات معينة على البيانات المدخلة للتأكد من صحة أوامر البرنامج، وذلك بتغيير مسار البرنامج إذا تم إدخال حرف (E) ضمن الأرقام المدخلة من لوحة المفاتيح إلى حقل معين. وقد اكتشف أحد مستخدمي النظام هذه الثغرة واستغلها بحيث استطاع إضافة مبالغ كبيرة إلى راتبه من خلال إدخاله لأجور إضافية وهمية.

٩ . ٢ . ٤ الفيروس المشفر

«الفيروس المشفر» هو ذلك الفيروس الذي يستطيع تشفير نفسه وفك شفرته مرة أخرى عند الحاجة. ويتكون هذا الفيروس من قسمين: أحدهما مشفر والآخر غير مشفر. مهمة القسم المشفر هي إخفاء وظيفة الفيروس

وإخفاء مفتاح التشفير السري الذي يستخدم في فك الشفرة، ومهمة القسم غير المشفر هي تشفير القسم المشفر أو فك شفرته.

وعندما يصيب الفيروس أحد البرامج يتولى القسم الخاص بالتشفير (وهو القسم غير المشفر) فك شفرة القسم المشفر (باستخدام المفتاح السري الذي تم توليده في آخر مرة تم فيها تشغيل الفيروس)، ومن ثم يقوم بتشغيل الفيروس ليبدأ العمل.

وبعد أن ينتهي الفيروس من أداء مهمته يقوم قسم التشفير بإعادة تشفير تعليمات الفيروس مرة أخرى (باستخدام مفتاح سري جديد في كل مرة)، ويمرر هذا المفتاح مع التعليمات المشفرة إلى القسم المشفر تمهيدًا لجولة أخرى لهذا لفيروس.

ويضمن هذا الأسلوب إخفاء جسم الفيروس ويجعله يبدو بشكل مختلف في كل مرة، ويظل قسم التشفير وحده بدون تغيير.

هدف المبرمج الذي يعد الفيروس المشفر هو ألا يترك سوى أقل عدد ممكن من التعليمات بدون تشفير، حتى لا يكشف عن هويته ووظيفته. هذه التعليمات هي ما نطلق عليه «توقيع الفيروس» (Virus Signature). ولحسن الحظ فإن البرمجيات المضادة للفيروسات تستطيع التعرف على هذا النوع من التوقيعات مهما كان حجمه صغيرًا، حتى لو كان هذا التوقيع مكونًا من مجرد عشرة أحرف.

٩ . ٢ . ٥ الفيروس متعدد الأشكال

«الفيروس متعدد الأشكال» (Polymorphic Virus) هو فيروس أكثر تعقيدًا من الفيروس المشفر فهو ينشئ في كل مرة يتوالد فيها قسم تشفير جديد يتولى عملية فك الشفرة، كما يستخدم في كل مرة مجموعة مختلفة

من التعليمات. وقد توصلت برمجيات مكافحة الفيروسات إلى إنشاء أسلحة جديدة فعالة لاستخدامها ضد هذه الفيروسات متعددة الأشكال (Nachenberg,1997).

٩ . ٣ مقاضاة صانعي الفيروسات

المكان: المملكة المتحدة . . الزمان: عام ١٩٩٥ . . . الحدث: أول محاكمة لمروج فيروسات . . الحكم: الإدانة.

كانت هذه هي أول سابقة من نوعها يسجلها تاريخ القضاء البريطاني بعد إجازة قانون إساءة استخدام الكمبيوتر في عام ١٩٩٠ . وتم تقديم المتهم إلى المحاكمة بعد التحقيقات التي أجرتها «سكوتلاند يارد».

وقد عرف هذا المجرم باسم « البارون الأسود»، وكان في السادسة والعشرين من العمر ومهنته مبرمج للحاسب الآلي، ولكنه كان متعطلاً عن العمل. وقد أدين بتهمة اقتحام بعض الحاسبات وزرع فيروسات الكمبيوتر فيها. ونتيجة لما قام به البارون الأسود خلال الفترة من أكتوبر ١٩٩٣ وحتى أبريل ١٩٩٤ ، وُجهت إليه إحدى عشرة تهمة بما فيها تهمة تحريض آخرين على زرع فيروسات مشفرة. وقد حازت الفيروسات التي زرعها على اهتمام منتجي برامج مكافحة الفيروسات في العالم كله عندما انتشرت خلال شبكة الإنترنت وطافت في منتهى السهولة بحاسبات العالم كله. وفي إحدى المرات قام البارون بتوزيع عينة من الفيروس من خلال لوحة الإعلانات (Bulletin Board) الخاصة بتبادل الفيروسات!.

وذكرت السلطات البريطانية أن تتبع الفيروسات التي نشرها وإصلاح الضرر الناجم عنها تكلف ما يربو على نصف مليون جنيه استرليني.

وفي عام ١٩٩٢ تحدثت وسائل الإعلام الأسترالية عن طالب في جامعة «كوينز لاند» ثبتت مسئوليته عن كتابة ونشر فيروسات الكمبيوتر التي عرفت باسم (Dudley) و (NoFrills) . ومنذ ذلك الوقت أصابت هذه الفيروسات في مناسبات متعددة مؤسسة «صن» وهي مؤسسة تأمين أسترالية كبيرة ومؤسسة الهاتف الأسترالية ومكتب الضرائب الأسترالي .

وفي عام ١٩٩٣ أُلقي القبض على صانع فيروسات بريطاني آخر وهو رئيس ما يُدعى «اتحاد الفيروسات شديدة الفتك» (ARCV) أو (Association of Really Cruel Viruses) وكانت التهمة الموجهة إليه هي الاحتيال على المكالمات الهاتفية .

وفي الولايات المتحدة تحدثت الصحف عن شاب لم يبلغ العشرين من عمره والذي اعترف بكتابة عدد من الفيروسات التي قام ضحاياه بنشرها بأنفسهم على نطاق واسع على شبكة الإنترنت دون أن يدركوا ذلك . وفي عام ١٩٩٣ هاجم فيروسه الخطير «الشيطان» (Satan Bug) شبكات المخابرات في الولايات المتحدة ، ومنذ ذلك الوقت فإن فيروسًا آخر من إنتاجه وهو «ناتاس» (Natas) ، وهي نفس حروف كلمة (Satan) معكوسة ، أصبح واحدًا من أكثر فيروسات الكمبيوتر شيوعًا في القارة الأمريكية . وحتى هذا التاريخ لم يتم تقديم أحد من صانعي هذه الفيروسات الخطيرة للمحاكمة .

٩ . ٤ الإنذار الكاذب عن الفيروسات

كثيرًا ما نسمع إنذارات كاذبة عن فيروسات لا وجود لها ، وتزدحم شبكة الإنترنت بأنباء عن فيروسات تغزو الشبكة بعضها صحيح وبعضها زائف . وهذه الإنذارات الكاذبة تستهلك وقت المستفيدين وجهدهم ، وهي بذلك ربما تصبح أشد خطرًا من الفيروات الحقيقية . ولعل فيروس «الأوقات

السعيدة» (Good Times) يعطي مثلاً واضحًا على ذلك حيث بدأ التحذير منه في عام ١٩٩٤ واستمر حتى هذه اللحظة. وهو يعتمد في انتشاره ليس على عدوى البرامج ولكن على انتقال الكلام من فم إلى فم.

وعادة تنجح هذه الإنذارات الكاذبة في إثارة الفزع إذا توافر فيها عنصران: الأول أن تتم صياغة الإنذار بلغة تبدو لغة تقنية علمية، والثاني أن تُنسب إلى مصدر موثوق به ولا يرقى إليه الشك. وفي هذه الحالة فإنها يمكن أن تخدع حتى المتخصصين، فنص الإنذار الكاذب بالفيروس الوهمي «الأوقات السعيدة» يقول: «إذا لم يتم إيقاف البرنامج فإن المعالج الخاص بالحاسب الشخصي سوف يدخل في حلقة تكرارية ثنائية لا نهائية مرفوعة للدرجة (ن)، والتي يمكن أن تلحق ضررًا بالغًا بالمعالج». وبرغم أن هذه اللغة تبدو مقنعة للوهلة الأولى إلا أننا بقليل من التمعن نستطيع أن نكتشف أنه لا يوجد شيء اسمه (حلقة تكرارية ثنائية لا نهائية مرفوعة للدرجة ن)، ومن المعروف أن معالجات الحاسبات الشخصية تم تصميمها لتنفذ حلقات تكرارية من تعليمات البرامج ويمكن أن تستمر في تنفيذها إلى الأبد دون أن يصيب المعالج أي ضرر أو تلف.

والمصدر الذي يُنسب إليه الإنذار يكون له تأثير كبير على القارئ، فلو أن عامل النظافة بشركة مايكروسوفت أرسل لصديق له إنذارًا بوجود فيروس خطير في «وندوز ٢٠٠٠» مثلاً فإن هذه الرسالة سوف يحملها الجميع محمل الجد.

٩ . ٤ . ١ الإنذارات الكاذبة شديدة الفتك

ربما كان أول إنذار كاذب بالفيروسات هو ذلك الذي حدث في أكتوبر ١٩٨٨ (Ferbrache,1992). ظهر هذا التحذير المسمى «فيروس المودم ٢٤٠٠ بود» من خلال مذكرة من «مايك روشنل» أحد مستخدمي الحاسب

ووصفت المذكرة هذا الفيروس بأنه (ربما كان أسوأ فيروس من فيروسات الحاسب الآلي ظهر في العالم حتى الآن). وشرح «روشنل» كيف اكتشف هذا الفيروس عندما دخل إلى إحدى اللوحات الإعلانية (Bulletin Boards) في جوف الليل حيث كان يحاول استرجاع بعض الملفات من هذه اللوحة الإعلانية، وبدلاً من عملية الاسترجاع المألوفة ادعى «روشنل» أنه فوجئ بفيروس أتلف القرص الصلب لجهاز الحاسب الشخصي الخاص به، ثم قام الفيروس بنشر نفسه عبر الموجة الحاملة (Carrier) التي يبثها المودم عند اتصاله بأجهزة المودم الأخرى على التردد ٢٤٠٠ بود أو أعلى. وكما يدعي «روشنل» فإن المودم بمجرد إصابته بالفيروس يقوم بنقل هذا الفيروس إلى أجهزة المودم الأخرى التي تستخدم موجة حاملة مشابهة، ومن ثم يلتصق هذا الفيروس بالبيانات التي تحملها هذه الموجات، وبمجرد وصول هذه البيانات إلى القرص الصلب فإن الفيروس يقوم بتدميره. وأضاف «روشنل» أنه لا توجد طريقة لإيقاف هذا الفيروس وإبطال مفعوله ومنعه من الانتشار سوى إعادة ضبط المودم على سرعة أقل! ولذلك ينصح «روشنل» كل المستفيدين بإنقاص سرعة المودم إلى ١٢٠٠ بود حيث أنها سرعة (آمنة)!!!.

إنذار كاذب آخر أطلقه في قالب ساخر «روبرت موريس الثالث»، وادعى مطلق الإشاعة أن هذا الفيروس يصيب أجهزة الحاسب من خلال مدخل الكهرباء للجهاز! وأنه يقوم بعكس اتجاه دوران القرص الصلب فتتم قراءة جميع البيانات معكوسة!!! وادعى أن هذا الفيروس قد أصاب ٣٠٠,٠٠٠ جهاز حاسب في ولاية «وست داكوتا» وحدها خلال ١٢ دقيقة فقط. وقدم موريس (إن كان هذا اسمه الحقيقي) النصائح التالية للمستخدمين، وليفترض القارئ العزيز وجود عدة علامات تعجب في نهاية كل من هذه النصائح:

- لا تستخدم الكهرباء لتشغيل الجهاز .
- لا تستخدم البطاريات كذلك حيث أن هناك شائعة تؤكد أن الفيروس قد غزا معظم مصانع البطاريات الكبرى وأنه يصيب القطب الموجب للبطارية (ولذلك يمكنك استخدام القطب السالب فقط) .
- لا تقم بتحميل أو استرجاع أية ملفات .
- لا تقم بتخزين الملفات سواء على القرص الصلب أو المرن ويمكنك استخدام أي وسيلة أخرى .
- لا تقرأ أي رسالة بريدية تستقبلها بما في ذلك هذه الرسالة .
- لا تستخدم المخرج المتتالي للحاسب أو المودم أو خطوط الهاتف .
- لا تستخدم لوحة المفاتيح أو شاشة الحاسب أو الطابعة .
- لا تستخدم وحدة المعالجة المركزية أو المعالجات الدقيقة أو الحاسبات المركزية .
- لا تستخدم الإضاءة الكهربية أو أجهزة التدفئة أو تكييف الهواء أو صنابير المياه أو الملابس الصوفية أو الدراجات .

٩ . ٥ الفيروس من الناحية الجنائية

من الملاحظ أن الفيروس المعلوماتي له من خصائص المجرم الكثير فهو يختفي كخطوة أولي إلى وقت محدد ثم يبدأ في الظهور كخطوة ثانية ليدمر في خطوة ثالثة ، تمامًا كالمجرم الذي يضع خطته لارتكاب الجريمة .

ويعاقب القانون الفرنسي كل من تسبب عمدًا ، ودون مراعاة لحقوق الآخرين ، في تعطيل أو إفساد تشغيل النظام . ومن هنا كانت أعراض الإصابة بالفيروس ذات آثار جسيمة جنائيًا .

وقد حدد المشرع عقوبة هذا الفعل بالحبس مدة تتراوح بين ثلاثة أشهر وثلاث سنوات ، والغرامة التي تتراوح من ١٠ آلاف فرنك إلي ١٠٠ ألف فرنك أو إحدى هاتين العقوبتين .

الفصل العاشر

المبرمجون وجرائم نظم المعلومات

المبرمجون وجرائم نظم المعلومات

نتعرض في هذا الفصل لمشكلة هامة تشكل صعوبة كبيرة لمسئولي أمن المعلومات، وتتسبب في الوقت نفسه في فتح ثغرات كثيرة ينفذ منها المتسللون والمجرمون لارتكاب جرائم نظم المعلومات، وهي أداء المبرمجين وممارساتهم الخاطئة وما يقعون فيه من أخطاء إما عفوية أو متعمدة. فنبدأ الفصل بالحديث عن بعض المصاعب التي تواجه مسئولي أمن المعلومات، مثل تعديل البرامج الأصلية المكتوبة بلغة المصدر، وكيف تُترك الصلاحيات لتتراكم لدى بعض المستفيدين والأساليب الخاطئة في منحها. ننتقل بعد ذلك لرصد بعض الممارسات الخاطئة للمبرمجين مثل التساهل في تقديم البيانات للبرامج الأخرى، وإهمال الاحتياطات اللازمة عند الانتقال إلى البيئة الإنتاجية، ثم نعطي مثالاً خطيرًا عن ثغرات البرامج ونتائج هذه الثغرات، ثم نتعرض لأخطر سقطات المبرمجين في التاريخ على الإطلاق ونعني بذلك «مشكلة القرن» (مشكلة عام ٢٠٠٠)، وهي مثال حي قاس للغاية على الممارسات الخاطئة للمبرمجين، ونوضح الجانب الآخر حيث أن هذه المشكلة لا تخلو من مزايا أمنية!.

نختتم هذا الفصل بالحديث عن بعض القضايا مثل قضية «من الذي يمتلك البرامج؟ . . المبرمج أم صاحب العمل؟ وقضية تأثير شكل المعلومات على أمن المعلومات، وتأثير الوسط الذي يحتوي على المعلومات على أمن هذه المعلومات.

١٠ . ١ مصاعب أمام مسئولي أمن المعلومات

١٠ . ١ . ١ تعديل البرامج الأصلية

يحتاج المختلس لإتمام جريمته إما أن يقوم بتعديل البرنامج الأصلي

المكتوب بلغة المصدر (Source program) أو بتعديل نسخته المترجمة بلغة الحاسب (Object program)، فإذا قام بتعديل البرنامج الأصلي فإنه يتعين عليه أن يخطو خطوة إضافية بترجمة هذا البرنامج إلى لغة الحاسب ليستطيع تحقيق غرضه. ومن السهل على المحققين في جرائم التزييف أو العاملين على منعها اكتشاف هذه التعديلات في البرامج الأصلية، بينما اكتشاف التعديلات في البرامج المترجمة يتطلب القيام بمقارنة مرهقة مع نسخة مترجمة سليمة من البرنامج.

١٠ . ١ . ٢ أخطاء منح الصلاحيات

من الأخطاء الشائعة في مراكز الحاسب الآلي عدم نزع الصلاحيات من الأشخاص الذين ينتقلون من مواقعهم إلى مواقع أخرى بل يتركون هؤلاء الأشخاص لتتراكم لديهم الصلاحيات عبر انتقالهم من منصب إلى آخر. ويزداد الأمر خطورة إذا صحب ذلك عدم الاحتفاظ بسجلات واضحة للصلاحيات.

كثيرًا ما نرى كيف يتم منح الصلاحيات للمستفيدين بناء على طلب من المستفيد يتم اعتماده من المدير المسئول، وذلك بدون سياسة ثابتة وواضحة ومخططة، وهذه من أكثر الأخطاء التي شاهدتها في كثير من مراكز الحاسب الآلي في الوطن العربي.

١٠ . ٢ ممارسات خاطئة للمبرمجين

١٠ . ٢ . ١ التساهل في تقديم البيانات للبرامج الأخرى

ينصح خبراء أمن المعلومات مبرمجي الحاسب الآلي بأنه عندما يقوم أحد البرامج بمناداة برنامج آخر فيجب أن يتيح البرنامج الأول للبرنامج

الثاني ما يحتاج إليه فقط من البيانات دون زيادة . ولكن بعض المبرمجين يجد من الأسهل أن (يدل) البرنامج المنادى على مكان البيانات (أي يشير إلى عنوانها) بدلاً من تجميع البيانات المطلوبة من أماكن وجودها مما يتيح للبرنامج المنادى بيانات أكثر من الحاجة ويفتح الباب بذلك لإضعاف أمن المعلومات . ولذلك فمن القواعد التي ينبغي اتباعها وعدم التساهل فيها عند كتابة البرامج أن يفترض كل برنامج سوء النية في باقي البرامج فأنت لا تعرف أي كود ضار سوف تتم إضافته إلى البرنامج الآخر .

١٠ . ٢ . ٢ الإهمال عند نقل البرنامج إلى البيئة الإنتاجية

يقوم بعض المبرمجين ببناء برامجهم بنفس أسلوب بناء العمارات الضخمة ، وهم خلال عملهم يكتبون بعض التعليمات التي تربط بين البرامج تمامًا مثل (السقالات) التي تصل بين أجزاء المبنى ، ومن ثم إزالتها في النهاية عند اكتمال العمل . ولكن من الممارسات الخاطئة للمبرمجين ترك هذه التعليمات والتغاضي عن إزالتها للاستفادة منها في إجراء التعديلات المستقبلية على البرنامج أو بغرض اختبار أداء البرنامج . هذه التعليمات (المنسية) والتي لا تكون مذكورة في العادة ضمن مواصفات البرنامج تصبح ثغرات أمنية مخيفة يمكن استغلالها أسوأ استغلال ونطلق عليها اسم «باب المصيدة» (Trapdoor) .

١٠ . ٢ . ٣ أخطاء البرمجة تسهل مهمة المتسللين

يمكن أن يتسبب المبرمجون في إيجاد ثغرات أمنية خطيرة إذا لم يهتموا بالتأكد من أطوال البيانات التي يقوم المستفيد بإدخالها في الحقول الثابتة . فإدخال بيانات أطول من استيعاب الحقل المدخلة إليه ينتج عنه دخول أجزاء من هذه البيانات في الحقول المجاورة ، مما يفتح الباب لثغرات أمنية كبيرة .

فقد يدخل المقتحم كلمة مرور مكونة من ستة عشر حرفًا في مكان كلمة المرور المكونة من ثمانية أحرف، فيقوم مثلاً بإدخال (ABCDEFGHABCDEFGH). في هذه الحالة تتعدى الكلمة المدخلة الحقل المخصص لها وتمتد لتحل محل كلمة المرور التي تتم المقارنة بها (بفرض أنها مجاورة للكلمة المدخلة)، وبذلك تتم مقارنة كلمتين متشابهتين معًا فتكون النتيجة أن يستطيع المقتحم الدخول بسهولة إلى الجهاز، وتتحطم أسوار الأمن.

وعند الحديث عن أخطاء المبرمجين نذكر خطأ ذلك المبرمج المتمثل في السهو عن إدراج «فاصلة منقوطة» في أحد البرامج المكتوبة بلغة (PL/1)، والتي كتبها أحد المبرمجين العاملين في وكالة الفضاء الأمريكية «ناسا». وكان هذا البرنامج مستخدمًا في توجيه إحدى مركبات الفضاء في العام ١٩٦٨، ونتج عن هذا الخطأ أن تاهت المركبة في الفضاء وضاعت على الوكالة ملايين الدولارات.

١٠ . ٢ . ٤ مثال خطير لثغرات البرامج

من أمثلة ثغرات البرامج التي تغري على استغلالها تلك الواقعة التي حدثت في عام ١٩٨٨ والتي أدين فيها أحد طلبة علوم الحاسب بارتكاب جريمة من جرائم نظم المعلومات، فقد اخترق هذا الطالب أحد البرامج وقام بتعديله وجعل منه ما يشبه برنامج «حصان طروادة» ثم أطلقه عبر شبكة الإنترنت. وانتشر هذا البرنامج بشكل مكثف من حاسب إلى آخر حتى أصاب أكثر من ستة آلاف جهاز كمبيوتر امتلأت جميعها بنسخ من هذا البرنامج، واضطر معظمها إلى التوقف عن العمل.

في هذه القضية استغل هذا الطالب ثغرة في برنامج «سند ميل» (Sendmail) وهو أحد نظم البريد الإلكتروني المجانية التي تُستخدم من

خلال نظام «يونكس»، وكان مصمم البرنامج الأصلي قد وضع هذه الثغرة عمدًا في البرنامج ولكن لهدف مشروع، وهو أن يسهل مهمة المبرمجين الذين قد يريدون إجراء التعديلات على هذا البرنامج في المستقبل. ويؤكد «باركر» أن هذا البرنامج (سند ميل) ما زال يستخدم بكثرة من جانب الكثيرين على شبكة الإنترنت دون أن يدروا بما فيه من ثغرات Parker,1998.

١٠ . ٢ . ٥ مشكلة القرن

مشكلة القرن، أو مشكلة عام ألفين، أو مشكلة الصفرين، وهي كلها مسميات لنفس المشكلة التي نعرفها جميعًا والتي ودعنا بها القرن العشرين، هذه المشكلة صاحبتها مشكلة أمنية أخرى ربما كانت أكثر خطورة، ومما زاد في خطورتها أن كثيرًا من الخبراء لم يلحظوها ولم يأخذوا حذرهم تجاهها. تتلخص هذه المشكلة في أن الشركات في اندفاعها المحموم لتعديل برامجها وتوفيق أوضاعها لتلائم الوضع الجديد كانت تستأجر مبرمجين متعاقدين لأداء هذه المهام دون التثبت من درجة الثقة بهم، وربما كان بعضهم غير أهل للثقة، فيقوم بإدراج بعض التعليمات الضارة ضمن البرامج (حصان طروادة مثلاً) ليتمكن فيما بعد من إلحاق الضرر بالشركة أو ابتزازها. ليس هذا فحسب، بل حتى مع مبرمجين موثوق بهم فإنهم في بعض الأحيان يتخلصون -بحسن نية أو قل بسذاجة- من الضوابط الأمنية الموضوعة داخل البرامج بهدف تسهيل العمل.

ولكن مشكلة القرن وما تم خلال علاجها لم يكن شرًا كله من الناحية الأمنية بل كانت له نواحي إيجابية، فالجهود المبذولة لتوفيق البرامج أدت في بعض الحالات إلى اكتشاف بعض الجرائم التي لولا هذا الفحص والتدقيق لما انتبه إليها أحد. ففي أكثر من حالة اكتشفت الشركات، خلال

عمليات تنقيح برامجها وإجراءاتها، جرائم كانت لا تزال ترتكب وتستنزف أموال الشركة. وتم هذا الاكتشاف لأن الكثير من هذه الجرائم كان يتطلب، لكي يستمر نجاحها، عدم تغيير البرامج أو الإجراءات.

وفي حالات أخرى انتهزت بعض المؤسسات فرصة إعادة النظر في البرامج والإجراءات لتحسين إجراءاتها الأمنية، أو إضافة إجراءات أمنية جديدة.

١٠ . ٣ من يمتلك البرامج؟

نود أن نناقش هنا قضية أراها في غاية الأهمية، وهي شعور المبرمجين بالاعتزاز الشديد بالبرامج التي يكتبونها والنظم التي يعدونها لدرجة الشعور بالامتلاك نحو هذه البرامج والنظم. وثارت الكثير من المشاكل وأقيمت الكثير من الدعاوى تتداولها ساحات المحاكم في كثير من دول العالم نتيجة لعدم حسم السؤال الهام: من الذي يمتلك البرامج؟ . . . المبرمج أم صاحب العمل؟ هل المالك هو المبرمج الذي أعد البرنامج وأنفق شهورًا طويلة في إبداعه؟ أم أن المالك هو صاحب العمل الذي مول العملية كلها بما فيها مرتب المبرمج نفسه؟ والمثال التالي يوضح حجم هذه المشكلة وأهمية حسمها.

قامت إحدى الشركات الصغيرة المتخصصة في برمجة الحاسب في إنجلترا بفصل إحدى المبرمجات العاملات لديها، ولكن الشركة لم تهتم بإلغاء صلاحيات هذه المبرمجة على الملفات المخزنة بحاسب الشركة. وبعد خروج المبرمجة من الخدمة قامت على مدى ساعات عديدة (١٨ ساعة) بالحصول على نسخ من البرامج المخزنة على حاسبات الشركة عبر شبكة الهاتف وتخزينها على حاسبها الشخصي في منزلها. وكانت نيتها، كما اعترفت بعد ذلك، هي استخدام هذه البرامج لتنشئ لنفسها شركة خاصة بها.

وكانت هذه المبرمجة قد قامت بكتابة (أو المشاركة في كتابة) الكثير من هذه البرامج وكان لديها الشعور بأن لها حقوقًا خاصة فيما يختص بهذه البرامج .

ولكن ما يهمنا في هذه القصة هو أن هذه الحقوق ، على فرض وجودها ، لابد أن تكون محددة ومدونة ضمن العقد الذي تبرمه الشركة مع موظفيها .

ولابد لنا أن نتساءل أين كانت نظم الرقابة ونظم تسجيل استخدام المعلومات؟ وأين كان مسئولو الأمن خلال هذه الفترة التي قضتها المبرمجة في الحصول على المعلومات من شبكة الشركة؟

١٠ . ٤ شكل المعلومة وأمن المعلومات

من منظور أمن المعلومات ، لا يتسبب تغيير حرف واحد أو رقم واحد في بيانات إحدى الصور (graphical data) في تحريف المعلومات التي تحتويها الصورة، كما لا يغير في قيمة الصورة، ولا يترتب على هذا التعديل خسائر كبيرة . بينما قد يتسبب تعديل حرف واحد، أو ربما رقم ثنائي واحد في حقل رقمي ، في تعديل أو ربما تدمير المعلومات التي يحتويها هذا الحقل ، وقد يتسبب عن ذلك خسائر لا يمكن توقعها . فشكل المعلومات إذًا، أو الصورة التي تكون عليها المعلومات ، له تأثير كبير في درجة الأمن التي تتطلبها هذه المعلومات .

ومن ناحية أخرى فتغيير الصورة التي تكون عليها المعلومة يمكن أن يؤثر في مدلول هذه المعلومة ، فلنفترض مثلاً أن موظفًا ساخطًا على المؤسسة قام بتشفير كل النسخ المتوفرة من ملف معين ثم أخفى مفتاح التشفير . كيف يمكن استعادة هذه المعلومات؟

يقودنا هذا لمناقشة درجة الأمن التي تتطلبها المعلومات المشفرة، فالمعلومات المشفرة تشفيرًا ضعيفًا يمكن كسره تحتاج إلى إجراءات لحمايتها ضد السرقة أو الاطلاع، بينما المعلومات المشفرة تشفيرًا قويًا فهي قد لا تحتاج أي إجراءات تأمين على الإطلاق.

برغم أننا عادة نحدد صلاحيات الاستخدام للموظفين على أساس الملف، إلا أننا نحتاج أحيانًا إلى تحديد صلاحيات خاصة لاستخدام بعض السجلات المعينة ضمن الملف أو حتى لبعض الحقول داخل السجل. في بعض الأحوال تمنح الإدارة موظفي إدارة شئون الموظفين صلاحيات الاطلاع على بعض سجلات الموظفين داخل الملف أو تعديلها، أو صلاحيات تعديل بعض الحقول داخل السجلات (مثل حقول العنوان أو الحالة الصحية أو مستوى الأداء في العمل أو غير ذلك).

وتلجأ بعض الشركات الكبيرة، لتحقيق مزيد من الأمن للبيانات، إلى فصل ملفات المديرين عن ملفات باقي الموظفين العاديين. بل قد تلجأ بعض هذه الشركات إلى حفظ ومعالجة هذه الملفات على حاسبات منفصلة.

١٠ . ٥ الوسط الذي يحتوي على المعلومات

المعلومات لابد لها من وسط يحتويها، حتى لو كان هذا الوسط هو مخ الإنسان، وقد يكون الورق هو هذا الوسط، أو قد يكون الوسط مغناطيسيًا كالأقراص المغنطة أو القرص الصلب في الكمبيوتر، ما قد يكون هذا الوسط عبارة عن كابلات تسري فيها نبضات. حتى الهواء الذي تسري فيه موجات كهرومغناطيسية تحتوي على المعلومات المنقولة هو أيضًا من وسائط المعلومات.

لكل نوع من أنواع وسائط المعلومات مخاطره الخاصة به، والإجراءات الأمنية المناسبة التي تحفظ المعلومات فيه من التلف أو الضياع أو الاطلاع غير المرخص به. ومن الشائع أن تكون إحدى وسائل المحافظة على المعلومات من الضياع هي إعداد نسخة أخرى منها على وسط مختلف، كأن نحتفظ بصورة ورقية للبرامج المخزنة على الحاسب، أو أن نحتفظ بشريط ممغنط به نسخة احتياطية من محتويات القرص الصلب. هذه النسخ، في بعض الأحوال، قد تكون قيمتها محدودة أو ربما تكون معدومة القيمة مثل الصور المنسوخة عن الأعمال الفنية الأصلية. ولكن عند نسخ بعض المعلومات على وسط مماثل للوسط الأصلي تكون قيمة النسخة تكاد تطابق قيمة الأصل.

أما على شبكة الإنترنت فالمعلومات يتم الاحتفاظ بنسخها في عدة أماكن، منها على سبيل المثال (الكمبيوتر الذي خرجت منه المعلومات، وبوابة الاتصال التي عبرتها المعلومات، وأجهزة الكمبيوتر الوسيطة التي انتقلت المعلومات عبرها أو انتهت عندها، وذاكرة الطابعة ووسائط النسخ الاحتياطي). وهنا تتعدد الوسائط، فنجد المعلومات تارة مخزنة على أقراص كبيرة (في الحاسبات المركزية) أو أقراص مرنة أو أقراص صلبة أو أشرطة أو على الورق. فالكتاب الذي بين يديك عزيزي القارئ بما فيه من صور ورسوم مخزن على ثلاثة أقراص لينة لا غير، ولديَّ من النسخ الإلكترونية للكتاب أكثر من عشر نسخ بين أقراص احتياطية ونسخ موجودة ضمن فهارس مختلفة على جهازي الخاص في المنزل أو الجهاز الخاص بي في العمل، وربما كان أيضًا مخزنًا في أكثر من نسخة لدى الناشر أو المصحح اللغوي أو الدار التي تولت التصميم والإخراج. وإذا فكرت في محو كل النسخ المخزنة من كتابي هذا فلابد لي أن أعرف أسماء جميع هذه الملفات والفهارس وأماكن وجودها!.

الفصل الحادي عشر

جدران الحماية

١١ . ١ جدران الحماية .

١١ . ٢ تصنيف جدران الحماية .

١١ . ٣ الموجه الحاجب .

١١ . ٤ الوسيط .

١١ . ٥ الحارس .

١١ . ٦ مقارنة أنواع جدران الحماية .

١١ . ٧ أمثلة على بنية جدران الحماية .

جدران الحماية

هذا الفصل خصصناه للحديث عن وسيلة مهمة من وسائل حماية المعلومات وهي «جدران الحماية»، فنبدأ بتعريف جدار الحماية، ثم تصنيف أنواع جدران الحماية وهي «الموجه الحاجب»، و«الوسيط»، و«الحارس». ثم نقارن بين هذه الأنواع، ونعطي أمثلة على استخداماتها. وننهي الفصل بالحديث عن كيفية تكوين جدران الحماية، وكيف يمكن أن نجمع بين أكثر من نوع منها معًا.

١١ . ١ جدران الحماية

١١ . ١ . ١ الحاجة إلى جدار حماية

هناك دائمًا تهديد قائم لجميع الشبكات الداخلية بالشركات والمؤسسات بأن مقتحمًا ما قد يخترق من خلال شبكة إنترنت نظامًا متصلاً بهذه الشبكة. ويكتسب هذا التهديد أهميته من أمرين: بينما لا تحتوي الرسالة الإلكترونية إلا على كمية محدودة من البيانات، لا تزيد عادة عن بضع مئات أو آلاف من الحروف، فإننا نجد النظم الأخرى المرتبطة بالشبكة تحتوي على ملايين بل مليارات الحروف أو أكثر من ذلك. الأمر الثاني هو أن المستفيد يدرك جيدًا احتمالات التعرض للاختراق عندما يقرر أن يرسل معلومات حساسة في رسالته، ويضع هذه الاحتمالات في اعتباره، ولكن مستخدمي النظم المرتبطة بشبكة محلية (LAN) على سبيل المثال ربما لا يدرون أن الحاسب الكبير الذي يستضيف شبكتهم مرتبط بشبكة أخرى واسعة النطاق (إنترنت مثلاً) ولذلك فهؤلاء المستخدمون قد لا يكونون على وعي بالتهديد القائم

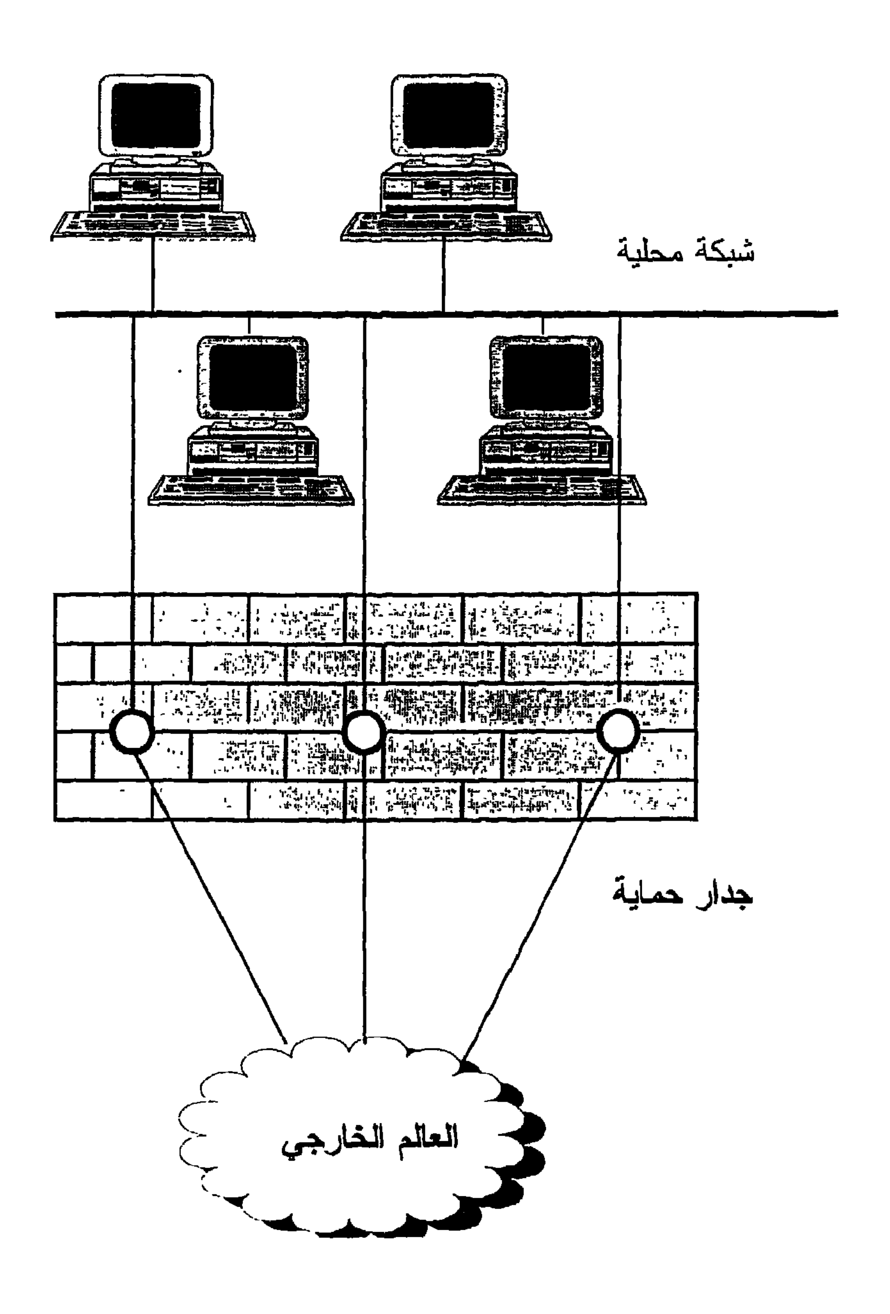
لكل بياناتهم المخزنة . ولذلك فإن حماية الموارد الأخرى لتلك الشبكات المرتبطة بإنترنت قد اكتسبت أهمية فائقة .

أبسط وسائل الحماية للموارد الحساسة هو عدم ربطها بأي نظام يمكن الوصول إليه من خارج المنظمة ، أو بعبارة أدق من خارج «الحدود الآمنة للمنظمة» ، وهذا العزل المادي فعال للغاية في مواجهة أخطار الاختراق الخارجي . ولكن العديد من المستفيدين يحتاجون ، وأكثر منهم يريدون ، الوصول إلى خارج هذه الحدود (لاستخدام إنترنت مثلاً) . وهنا ربما يقوم أحد المستفيدين بشراء جهاز مودم رخيص الثمن ويقوم بتركيبه في حاسبه الشخصي الموجود في مكتبه والمرتبط بشبكة المنظمة المحلية ، ثم يقوم المستفيد بالاتصال بالخارج عن طريق الهاتف الموجود بمكتبه . هذه الممارسة ربما تكون في غاية الخطورة لأن مسئولي أمن المعلومات لا يعرفون بوجود هذا المودم وبالتالي فهم لا يستطيعون مراقبته أو نصح المستفيد عن كيفية تقليل درجة التعرض لخطر الاختراق ، وهم بالطبع لن يقوموا ببناء دفاعات لحماية باقي موارد المنظمة المتصلة بهذا المستفيد الشارد . هذه المنظمة إذن في حاجة إلى مصفاة (فلتر) لا تسمح بالمرور إلا للاتصالات المرغوب فيها فقط وتمنع ما عداها . وفي الوقت نفسه يجب ألا تعوق هذه المصفاة عمليات المستفيد وألا تحرمه من الأنشطة التي يرغب في القيام بها حتى يقتنع هذا المستفيد بعدم الحاجة إلى شراء المودم الخاص به الأمر الذي لو تم قد يفشل مهمة هذه المصفاة تمامًا . هذه المصفاة المطلوبة تشبه كثيرًا قلاع العصور الوسطى ، تلك القلاع التي كانت لها أسوار عالية وقوية تتخللها فتحات ضيقة يستطيع الرماة من خلالها إطلاق أسهمهم على الأعداء . وكانت هذه الفتحات من الضيق بحيث يكاد يكون من المستحيل استخدامها من جانب العدو في إطلاق أسهمه من الخارج إلى الداخل . هذا النوع من الدفاع يُسمى «جدار الحماية»

(Firewall). فجدار الحماية في ذلك الزمان كان حائطًا من الحجارة تتخلله فتحات صغيرة بهدف التحكم بدقة فيما يمر من خلال هذه الفتحات (داود، ٢٠٠٠).

١١ . ١ . ٢ ما هو جدار الحماية؟

جدار الحماية هو أداة تصفي (أو تحجز) مرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية التي نخشى منها، والهدف منه هو حجز كل ما هو غير مرغوب فيه خارج البيئة المحمية. ولابد أن يطبق جدار الحماية المستخدم سياسة أمنية معينة، هذه السياسة قد تكون مثلاً منع أي دخول من الخارج مع السماح بالمرور من الداخل إلى الخارج. أو قد تكون هذه السياسة السماح بالدخول من أماكن معينة فقط أو من جانب مستفيدين معينين أو تسمح بالدخول لأنشطة معينة فقط دون باقي الأنشطة. ويعتبر وضع السياسة الأمنية السليمة التي تلبي احتياجات المنظمة هو أحد التحديات الحقيقية التي تواجه المنظمة عندما تقرر حماية شبكتها عن طريق جدار الحماية.



شكل (١١ ـ ١) جدار الحماية Firewall (داود ٢٠٠٠)

١١ . ٢ تصنيف جدران الحماية.

هناك عدة أنواع من جدران الحماية من بينها :

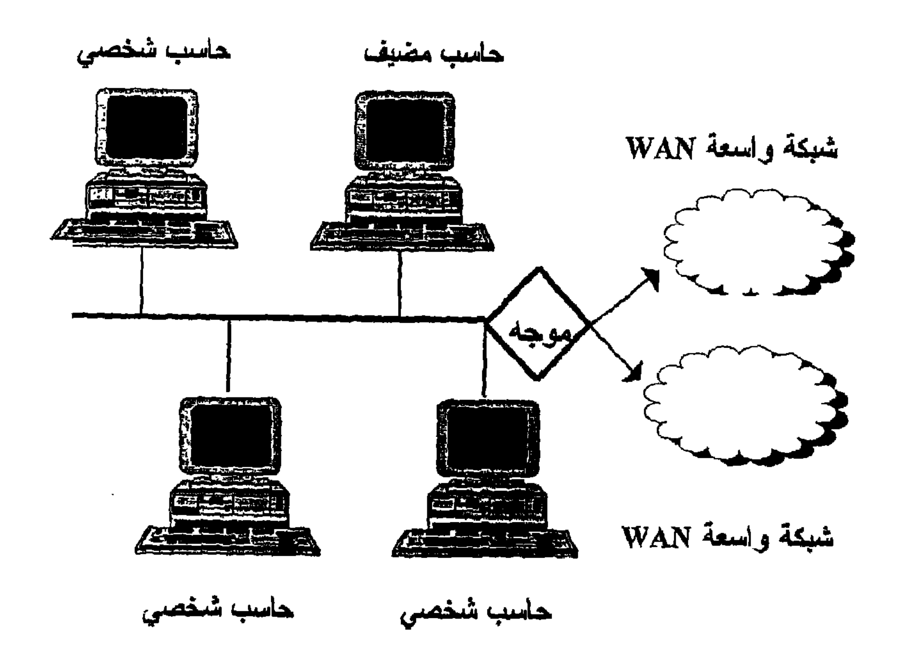
- الموجه الحاجب Screening Router .
- الوسيط Proxy .
- الحارس Guard .

وهذه الأنواع تختلف عن بعضها في الإمكانيات وفي مجالات الاستخدام، ولكن ليس من الضروري أن يكون أحدها أفضل من الآخرين، وبصفة عامة فالموجه الحاجب يتجه لتطبيق سياسات أمنية أكثر بساطة أما الوسيط والحارس فيمكن من خلالهما الاختيار من بين العديد من السياسات الأمنية التي يمكن اتباعها . والبساطة في السياسة الأمنية ليست عيبًا، وإنما اختيار النوع المناسب من جدار الحماية يتوقف على طبيعة الأخطار أو التهديدات التي تحتاج المنظمة إلى مواجهتها .

جدار الحماية لا يعدو كونه مجرد حاسب عادي، فالموجه الحاجب يمكن أن يكون حاسبًا بسيطًا جدًا ولكن الاتجاه هو أن تستخدم هذه الموجهات حاسبات كاملة ذات نظام تشغيل مستقل لأن برامج التحرير (Editors) وغيرها من الأدوات مطلوبة لمساعدة المستفيد في تصميم وصيانة الموجه، وعلى أي حال فمطورو جدران الحماية يتجهون دائمًا إلى التبسيط واللجوء باستمرار إلى حذف كل الإمكانيات والتسهيلات والبرامج غير الضرورية من جدار الحماية، والسبب هو منع تقديم أي مساعدة للمهاجم الذي ينجح في الاقتحام، ولهذا السبب بالذات تتجه جدران الحماية لعدم الاحتفاظ ببيانات المستفيدين فهي لا تحتوي مثلاً على ملف كلمات المرور . وفيما عدا عمليات المراجعة الدورية لقوائم المراقبة التي يتابعها جدار الحماية فلا يوجد سبب لاستخدامه أو التعامل معه فلديه مهمة تستغرق كل إمكانياته التي يجب أن تظل مخصصة لهذا الغرض .

١١ . ٣ الموجه الحاجب Screening Router

الموجه الحاجب هو أبسط أنواع جدران الحماية وفي بعض المواقف يكون هو أكثرها فاعلية . نعرف أن الحاسبات «المضيفة» (Hosts) ليس من المستحب في العادة توصيلها مباشرة بالشبكات الكبيرة (WANs) ولكنها تتصل بهذه الشبكات من خلال «موجه» (Router) وهو بدوره عبارة عن حاسب يقوم، بتوجيه الرسائل إلى وجهتها، فالموجه تتلخص مهمته في استقبال حزم الرسائل (Packets) وبناء على جداول التوجيه المخزنة لديه يقوم بتمرير الحزمة الواردة إلى أحد المنافذ العديدة التي تتولى بدورها إيصال كل حزمة إلى وجهتها كما يبين الشكل (١١ - ٢) .

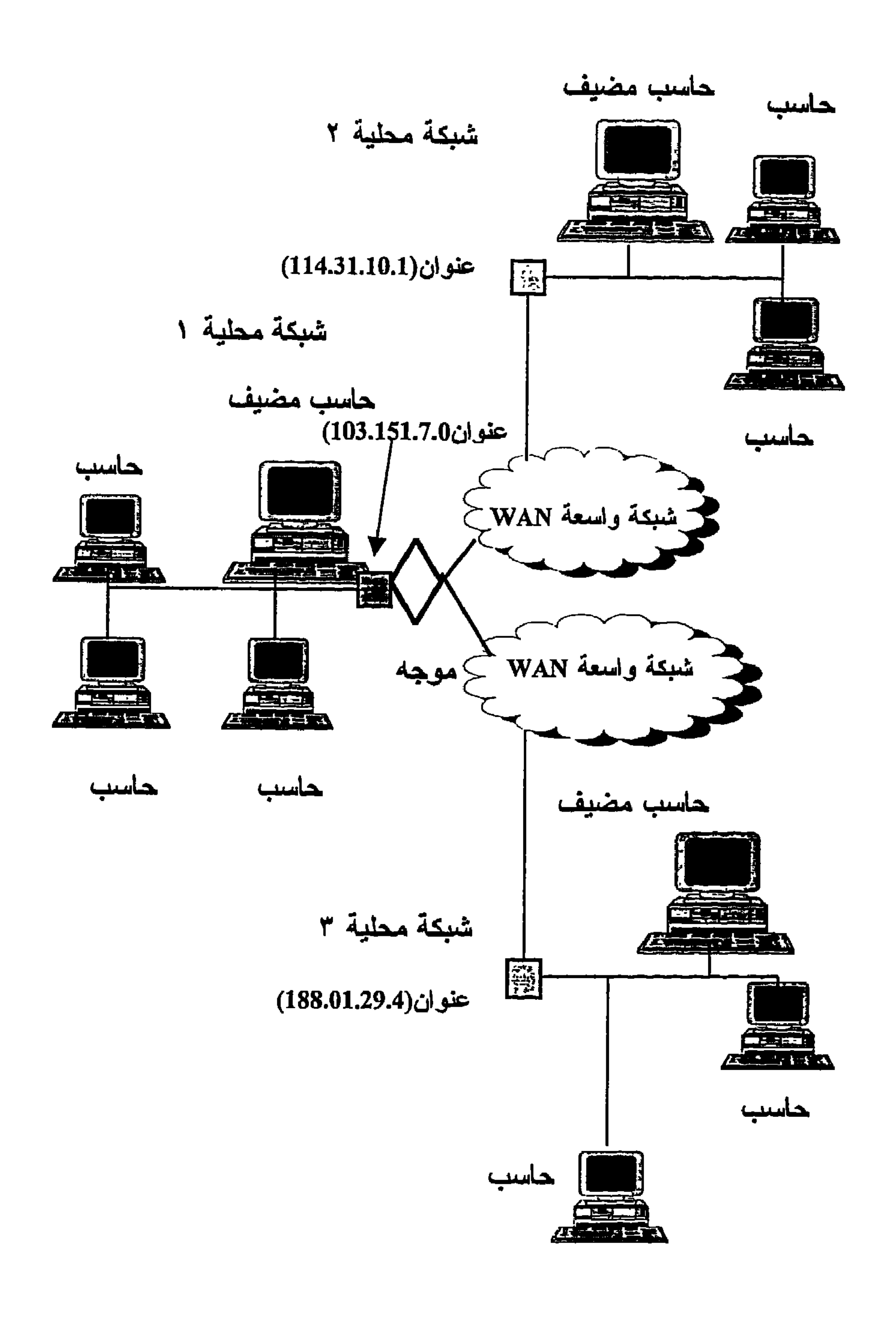


شكل (١١-٢) «موجه حاجب» (Screening Router) يصل شبكة محلية بشبكات واسعة

ويعمل الموجه عادة في كلا الاتجاهين فيقوم بتمرير حزم البيانات الآتية من الشبكة الداخلية وبثها إلى العالم الخارجي ، كما يستقبل الحزم الواردة من الخارج ويمرر تلك الحزم إلى العناوين المرسلة إليها في الشبكة الداخلية . ولنأخذ المثال التالي : شركة عالمية لها ثلاث شبكات محلية في ثلاثة مواقع حول العالم كما يبين الشكل (١١ - ٣) .

في هذه الحالة نختار موقع الموجه بحيث تكون الشبكة المحلية في المركز الرئيسي على أحد جانبي الموجه (الجانب الداخلي) بينما تقع الشبكتان البعيدتان على الجانب الخارجي لهذا الموجه ، حيث يتم الوصول إليهما عبر شبكة واسعة (WAN) ولتكن شبكة إنترنت مثلاً .

قد تكون السياسة الأمنية لهذه المنظمة هي أن تقتصر الاتصالات بين هذه الشبكات الثلاث عليها وحدها دون السماح بتبادل البيانات بينها وبين أي شبكات أو أجهزة أخرى . هنا يمكن استخدام أسلوب الموجه الحاجب بتركيبه على الشبكة الأولى مثلاً وليكن عنوانها هو (٠ . ٧ . ١٥ . ١٠٣)، وتكون مهمة هذا الموجه الحاجب هي عدم السماح (بالخروج) إلا للاتصالات التي تكون وجهتها العنوان (٤ . ٢٩ . ٠١ . ١٨٨) أو العنوان (١ . ١٠ . ٣١ . ١١٤) وهي عناوين الحاسبات المضيفة للشبكتين الأخريين .



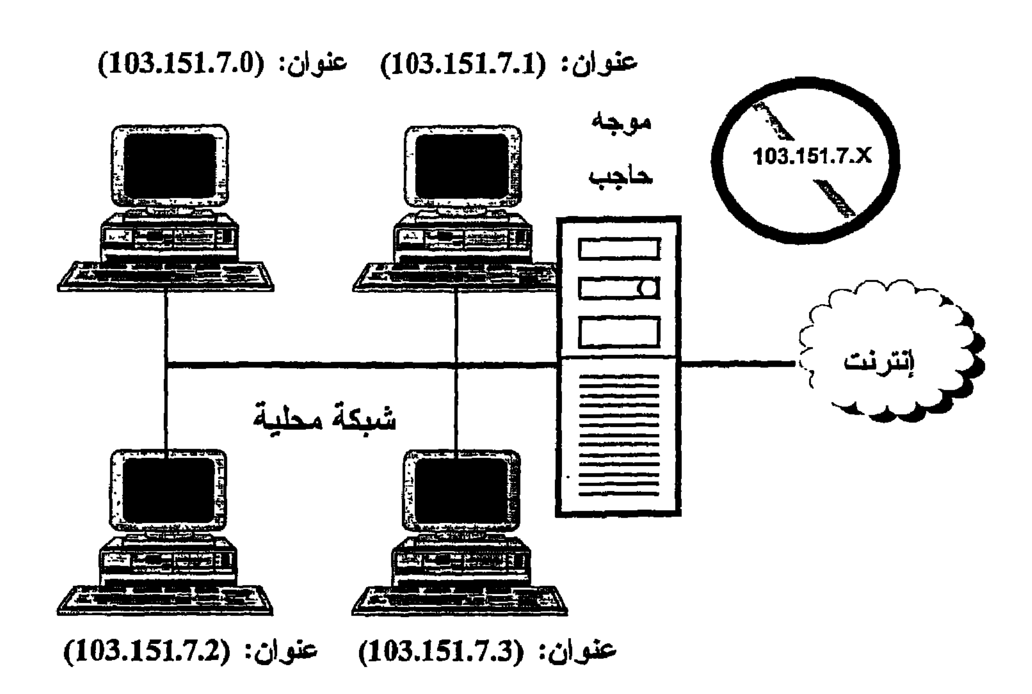
شكل (١١ ـ ٣) ثلاث شبكات محلية مرتبطة

نلاحظ أن هذه التصفية تتم على مستوى الحزمة أي على مستوى تفصيلي جدًا، فالحزمة هي وحدة صغيرة جدًا من البيانات المتبادلة لا تزيد عن بضع مئات من الحروف، وحيث إن الموجه قد يكون عليه أن يمرر آلاف الحزم في الثانية الواحدة؛ لذلك فإن قواعد الحجب أو السماح لا بد أن تكون قواعد بسيطة يستطيع الموجه أن يختبرها ويطبقها بسرعة كبيرة دون أن تتأثر حركة مرور البيانات، كما إن تصميم الموجه يجب أن يتم بحيث ينظر إلى المعلومات الموجودة في مقدمة الحزمة فقط (Header) وليس محتويات الحزمة نفسها.

وحسب البروتوكول المستخدم فإن المقدمة عادة تحتوي على كل من «عنوان المصدر»، و»عنوان الوجهة»، و«البروتوكول المستخدم»، و»مَنْفذ الإرسال»، و»مَنْفذ الوصول»، وعدد حروف الحزمة، وترتيب الحزمة داخل الرسالة، والأولوية، وبعض المعلومات الأخرى التي يتم تضمينها خصيصًا لاكتشاف أخطاء الإرسال. ومن ثم فهذه البيانات هي فقط التي يمكن للموجه اختبارها واتخاذ قرار بشأنها وليس محتوى الرسالة وما قد تتضمنه من معلومات أو كلمات معينة قد نرغب في استبعادها.

هذه الموجهات الحاجبة تستطيع أداء مهمة على جانب كبير من الأهمية وهي التأكد من صحة العناوين الداخلية أي عناوين الحاسبات المضيفة داخل الشبكة الداخلية للمنظمة، فالسبيل الوحيد الذي يجعل الحاسب المضيف يتمكن من تمييز حاسب مضيف آخر هو العنوان المبين في حقل المصدر بالرسالة، ولكن عناوين المصدر في حزم البيانات قابلة للتزوير، ولذلك فربما ينخدع أحد التطبيقات المحلية في المنظمة بالعنوان المزور ويظن أنه يتعامل مع حاسب مضيف آخر ضمن الشبكة الداخلية وليس مع مزور من الخارج، ولما كان الموجه يقع في موقع متوسط بين الشبكة الداخلية والشبكة الخارجية فهو

لهذا يستطيع اكتشاف إذا ما كانت هذه الحزمة الآتية من الخارج تدعي أنها صادرة من الداخل أم لا وذلك عن طريق التحقق من أن عنوان المصدر ليس أحد عناوين المصدر للحاسبات المضيفة الداخلية كما يبين شكل (١١ - ٤).



شكل (١١-٤) «موجه حاجب» يحجب بعض العناوين الخارجية

ويمكن بناء «الموجه الحاجب» بحيث (يحجز) جميع الحزم الواردة من (الخارج) والتي تدعي لنفسها عنوان مصدر ضمن عناوين المصدر الداخلية، ففي هذا المثال يحجز الموجه كل الحزم الواردة من الخارج والتي يكتشف أن حقل عنوان المصدر فيها هو (X.٧ . ١٥١ . ١٠٣).

يستطيع الموجه الحاجب كذلك أن يتحكم في المرور عن طريق التطبيق (في طبقة التطبيقات)، فالعنوان الذي يراه الموجه هو في حقيقته مكون من جزأين: الجزء الأول هو عنوان الشبكة والثاني هو «رقم منفذ التطبيق». والتطبيقات القياسية مثل «بروتوكول نقل الملفات» (FTP) أو «البروتوكول البسيط لنقل البريد» (SMTP) لها أرقام منفذ قياسية (الأول رقمه ٢١ والثاني رقمه ٢٥). ويظهر رقم المنفذ في عناوين المصدر والوجهة بالحزمة، فمن العنوان (٣٢٥ . ٢٥ . ٥٠ . ٠٠) نفهم أن البروتوكول المستخدم هو بروتوكول (SMTP). ويمكن تصميم الموجه الحاجب بحيث يسمح مثلاً بمرور الحزم من الداخل إلى الخارج فقط، أو من الخارج إلى الداخل فقط.

١١ . ٤ الوسيط : Proxy

علمنا أن الموجهات الحاجبة لا تنظر إلا إلى مقدمات الرسائل فقط وليس للمحتوى ولذلك فهي قد تمرر أي رسالة للمنفذ رقم ٢٥ مثلاً إذا كانت قواعد الحجب تسمح بمرور الرسائل إلى هذا المنفذ، ولكن بعض شركات تقديم خدمة توصيل البريد الإلكتروني قد تحتاج أحيانًا للتصرف بالنيابة عن المستفيدين (لتخزين البريد الوارد مثلاً حتى يستطيع المستفيدون الرجوع إليه لاحقًا أو التأكد من صحة بعض الرسائل) وربما تود المنظمة نفسها فحص البريد الوارد إليها قبل السماح بمروره إلى الداخل. هنا يأتي دور «الوسيط» (Proxy)، ويسمى أحيانًا «الحاسب المنيع» (Bastion host) وهو عبارة عن

نوع من جدران الحماية يقوم بفحص الطلبات الواردة للنظام بحيث لا يتلقى هذا النظام سوى الطلبات السليمة فقط، فالوسيط هنا عبارة عن برنامج يعمل كعملة ذات وجهين: من الداخل نرى هذا البرنامج كما لو أنه كان هو الجه المتصلة من الخارج، بينما يتصرف هذا البرنامج من الخارج في مواجهة الجهة الخارجية تمامًا كما يجب أن يفعل المتصل الداخلي.

عندما يتم نقل البريد الإلكتروني من موقع إلى آخر فإن عملية الإرسال وعملية الاستقبال تتمان عن طريق بروتوكول واحد يتم اختياره بعناية، يقوم هذا البروتوكول بالتحقق أولاً من شرعية العملية، ثم يتولى نقل الرسالة بالفعل. يتدخل «الوسيط» (Proxy) خلال هذا التبادل البروتوكولي بحيث يبدو بالنسبة للمرسل الموجود خارج جدار الحماية كما لو كان هو نفسه المستقبل الداخلي، ويبدو بالنسبة للجهة الحقيقية المستقبلة داخل المنظمة كما لو كان هو المرسل الخارجي.

والوسيط هنا في موقعه المتوسط لديه الفرصة لحجب البريد المرفوض (المرسل وفقًا لبروتوكول آخر مثلاً) للتأكد من أن تلك الأوامر التي تم إرسالها إلى الجهة المستقبلة هي أوامر تابعة للبروتوكول المحدد فقط. وهذه الخاصية يمكن استغلالها بشكل جيد لتحقيق الكثير من متطلبات أمن المعلومات.

١١ . ٤ . ١ أمثلة على استخدام الوسيط.

لكي نفهم الغرض الحقيقي من استخدام الوسيط نضرب بعض الأمثلة التي يتطلب تحقيقها استخدام الوسيط:

١ ـ شركة تريد إنشاء قائمة أسعار يطلع عليها العملاء مباشرة (Online) بحيث يمكن لأي شخص من خارج الشركة أن يرى المنتجات التي تقدمها الشركة وأسعارها. وتريد هذه الشركة التأكد من عدم استطاعة أي شخص من

خارج الشركة أن يقوم بتغيير هذه الأسعار أو المنتجات، وأن المتصلين من الخارج لا يستطيعون الوصول إلا إلى قائمة الأسعار هذه فقط وليس إلى أيٍّ من الملفات الحساسة المخزنة في شبكة الشركة الداخلية.

٢ - مدرسة تريد السماح لطلبتها بالحصول على المعلومات التي يحتاجون إليها من «الشبكة العنكبوتية» (World Wide Web) أو (WWW) من خلال إنترنت، ولكي تتمكن المدرسة من تقديم خدمة أفضل لطلبتها فهي تريد معرفة المواقع التي تمت زيارتها من قبل الطلبة والملفات التي قام الطلبة بالحصول عليها من هذه المواقع، وذلك حتى تقوم المدرسة لاحقًا بالحصول على نسخة من الملفات التي يتبين أنها تُسترجع بصفة مستمرة ومن ثم تتيح هذه الملفات داخليًا، وذلك باستخدام أسلوب «الذاكرة الخبيئة» (Cache) بحيث لا يحتاج الطلبة إلى شغل الشبكة للحصول عليها.

٣ - منظمة حكومية تحتفظ ببيانات إحصائية متاحة لاستخدام المواطنين، وتريد أن تجعل هذه المعلومات في متناول المواطنين وحدهم دون غيرهم، ولذلك فالحكومة تريد تطبيق هذه السياسة عن طريق السماح بالوصول إلى هذه البيانات من جانب العناوين التي تقع داخل الدولة فقط وعدم السماح بالوصول إليها من خارج الدولة.

٤ - شركة لديها مكاتب متعددة وتود تشفير محتويات جميع البريد الإلكتروني المتبادل بين مكاتبها، في هذه الحالة يلزم وجود «بوابة للتشفير» وبوابة أخرى لفك الشفرة في كل موقع.

٥ - تريد إحدى الشركات السماح باستخدام موظفيها للحاسب الآلي الخاص بها عن طريق الاتصال الهاتفي من منازلهم، دون تعريض موارد الشركة لتطفل الآخرين من الخارج من غير موظفي الشركة.

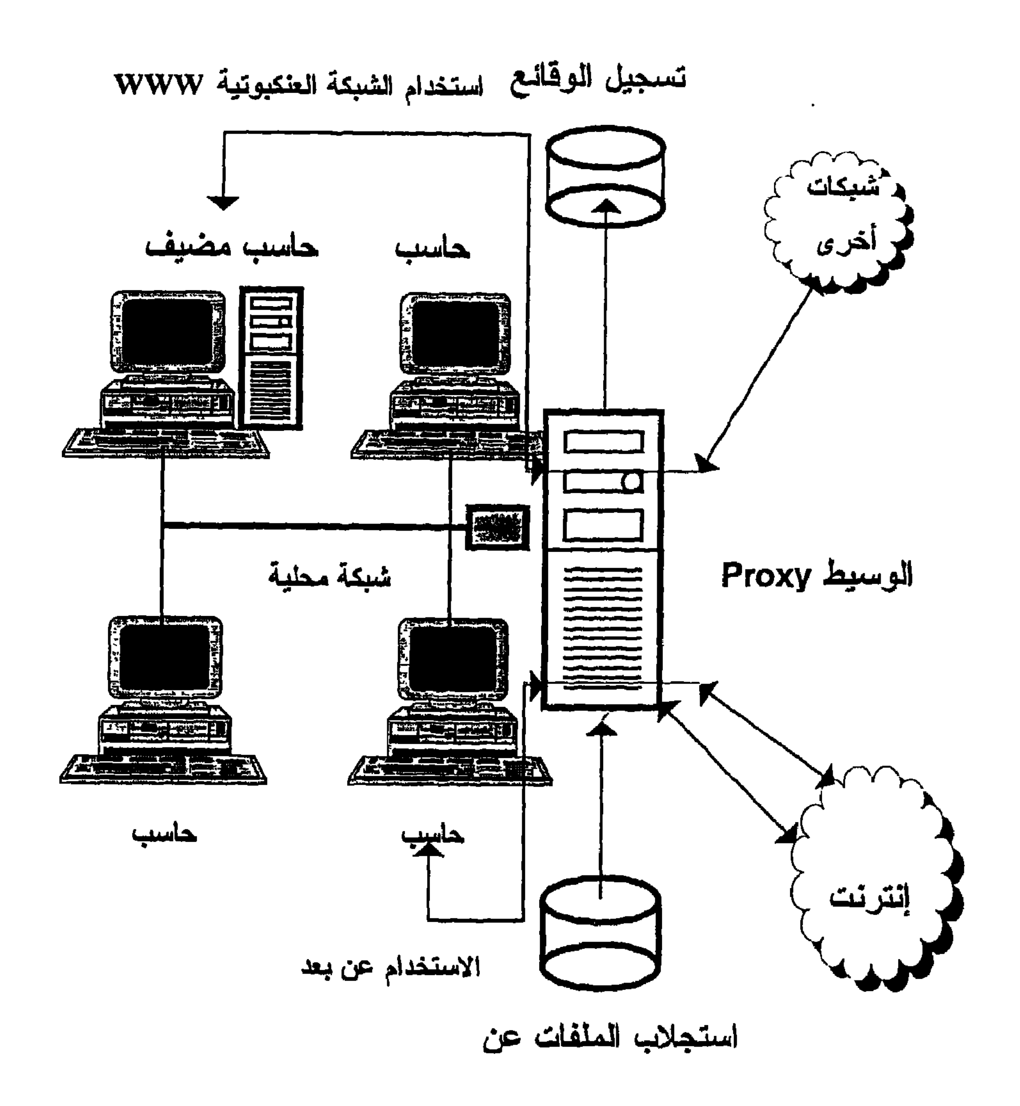
كل من هذه الاحتياجات يمكن تحقيقه عن طريق الوسيط، ففي الحالة الأولى يمكن للوسيط أن يراقب بيانات بروتوكول نقل الملفات للتأكد من أن ملف قائمة الأسعار وحده هو الذي يتم طلبه أو الدخول إليه وأن البروتوكول يسمح بالقراءة فقط من هذا الملف وليس بتعديله، واحتياجات المدرسة يمكن تلبيتها عن طريق استخدام برنامج فرعي لتسجيل الوقائع (Logging) كجزء من البرنامج «المتصفح» (Browser). أما طلب المنظمة الحكومية فقد كان من الممكن تحقيقه عن طريق موجه حاجب، ولكن برمجة جدار الحماية الوسيط عادة ما تكون أكثر مرونة وأكثر قابلية للتحكم فيها. والحاجة إلى تحديد الأشخاص المسموح لهم بالدخول إلى النظام (Login) يمكن تحقيقها عن طريق برمجة الوسيط من خلال برنامج تتم كتابته خصيصًا بحيث يطلب من المستفيد تعريفًا دقيقًا بشخصيته. ويبين الشكل (١١ ـ ٥) بعض إمكانيات جدار الحماية الوسيط.

جدار الحماية الوسيط يكون عادة جهاز حاسب مستقلاً معزولاً، وتكون إمكانيات هذا الحاسب محدودة للغاية، ومن المهم جدًا ألا يُسمح بدخول المستفيدين إليه (برغم أنه قد يُسمح لهم من خلاله بالدخول إلى الشبكة الداخلية للمنظمة) وذلك حتى لا تُتاح الفرصة لأي متطفل لإجراء أي تعديل على القواعد المبرمجة داخله. وهذا الجهاز يجب ألا يحتوي على أي برامج أخرى غير ضرورية للغرض الذي أنشئ من أجله. وبهذا التضييق الشديد على الإمكانيات البرمجية لهذا الجهاز يمكن التأكد من أنه لا توجد ثغرات يمكن الاختراق من خلالها، ولن يجد المقتحم الذي قد يتمكن من الوصول إليه أي مساعدة تذكر تمكنه من تنفيذ أي عملية غير مشروعة.

هذه البرمجيات التي تنظم عمل جدار الحماية الوسيط يمكن تعديلها بحيث تلائم بعض الاحتياجات الخاصة للمنظمة مثل تسجيل تفاصيل كل

الاتصالات التي تتم أو تسجيل عمليات الدخول التي تتم من خارج المنظمة . بل يمكنها كذلك أن تجعله يعرض واجهة مستفيد عامة تظهر لكل متصل تحدد الوظائف التي يستطيع المتصل الخارجي القيام بها ، ولا تظهر هذه القائمة بعض العمليات التي ربما لا نرغب في قيام المتصل الخارجي بتنفيذها على النظام . فبفرض أن الشبكة الداخلية للمنظمة تضم عدة حاسبات مضيفة مركب عليها نظم تشغيل مختلفة وبفرض أن هذه النظم جميعها ليست لديها القدرة على التمييز الدقيق لشخصية المتصل ، فبرنامج الوسيط في هذه الحالة يكون دوره أن يطلب التعريف المطلوب من المتصل (الاسم وكلمة السر وأي معلومات أخرى للتأكد من شخصيته) ومن ثم يتحقق من شخصية المتصل بنفسه وبعد ذلك يمرر للحاسب المطلوب الاتصال به فقط الاسم وكلمة السر بالشكل المطلوب لنظام التشغيل المركب على هذا الحاسب .

الميزة التي يتفوق بها الوسيط على الموجه الحاجب هي أن الوسيط يستطيع أن يفهم ويفسر البروتوكول المستخدم وذلك بهدف التحكم في التصرفات المسموح بها من خلال جدار الحماية بناء على بعض المحددات داخل البروتوكول وليس مجرد بيانات المقدمة الخارجية فقط .



شكل (١١- ٥) وظائف متعددة للوسيط Proxy

١١ . ٥ الحارس Guard

«الحارس» هو حائط نار يشبه الوسيط (أي أنه مبرمَج) إلا أنه على درجة كبيرة من التعقيد، وهو يتقبل وحدات بيانات البروتوكول ويفسرها، وبناء على تفسيره هذا إما أن يسمح بمرورها كما هي أو يقوم بتمرير وحدات أخرى بديلة للحصول على نتائج أخرى.

و«الحارس» يقرر بنفسه ما هي الخدمات التي يجب أن يؤديها نيابة عن المستفيد وذلك اعتمادًا على المعلومات المتاحة: مثل ما إذا كان يستطيع التعرف على شخصية المستفيد الخارجي أو تحديد التعاملات السابقة معه مثلاً، ودرجة التحكم التي يستطيع الحارس توفيرها محدودة بما يمكن حسابه أو استنتاجه. ولا يوجد هناك تحديد حاسم يفصل بين الحارس والوسيط سوى درجة تعقيد البرنامج، فإذا زاد تعقيده كثيرًا أمكن اعتباره حارسًا.

١١ . ٥ . ١ أمثلة لنشاط «الحارس»

فيما يلي بعض الأمثلة الأكثر تعقيدًا لنشاط الحارس:

١ - إحدى الجامعات تود السماح لطلبتها باستخدام البريد الإلكتروني ولكن إلى حد معين، أي لا يجب أن يتعدى البريد الذي يرسله الطالب عددًا معينًا من الرسائل، أو لا يجب أن يتعدى حدًا أقصى من عدد الحروف في اليوم الواحد أو خلال الأسبوع مثلاً. برغم أن هذه النتيجة يمكن الحصول عليها عن طريق تعديل البرنامج الذي يتم من خلاله إرسال البريد الإلكتروني إلا أنه في هذه الحالة ربما يستطيع أحد الطلبة استخدام أكثر من نسخة من برامج البريد لتجاوز هذا القيد، ولذلك يمكن تحقيق سهولة أكثر وكفاءة أعلى عن طريق مراقبة النقطة المشتركة التي يمر من خلالها كل البريد الإلكتروني للمنظمة ألا وهي «بروتوكول نقل البريد» (Mail Transfer Protocol).

٢ ـ مدرسة تريد تمكين طلبتها من استخدام «الشبكة العنكبوتية» (WWW)، ولكن بسبب السرعة البطيئة للوصلة التي تستخدمها المدرسة للاتصال بهذه الشبكة فإنها تود أن تسمح لطلبتها بكمية محدودة من البيانات المنقولة خلال عمليات «استجلاب الصور» (Image Downloading) (أي بالسماح باستجلاب النصوص والرسوم البيانية البسيطة فقط مع منع الرسوم المعقدة والرسوم المتحركة والقطع الموسيقية وما إلى ذلك).

٣ ـ مكتبة تريد أن تتيح بعض الوثائق لمرتاديها، ولكن لكي تضمن عدم انتهاك حقوق الملكية الفكرية فإنها تريد السماح للمستفيد باسترجاع عدد معين من الكلمات التي تبدأ بها الوثيقة، ولكن بعد الوصول إلى هذا الحد يجب على المستفيد أن يدفع رسومًا معينة تقوم المكتبة بدفعها لصاحب حقوق الملكية الفكرية.

٤ ـ شركة تريد السماح لموظفيها بالحصول على ملفات عبر «بروتوكول نقل الملفات» (FTP)، ولكن من أجل منع دخول الفيروسات إلى شبكة الشركة فإنها تريد تمرير كل الملفات الواردة من خلال برنامج فحص الفيروسات. وبرغم أن معظم هذه الملفات سوف يكون نصوصًا أو رسومًا غير قابلة للتنفيذ إلا أن إدارة الشركة رأت أن تكلفة فحص هذه الملفات لن تكون ذات قيمة تذكر.

كل من هذه «السيناريوهات» يمكن تنفيذه عن طريق «الوسيط» بعد تعديل البرنامج، ولكن لأن قرارات البرنامج ليست بسيطة ولأنها تعتمد على نوعية البيانات المنقولة وتتطلب فحصًا للبيانات الواردة أو المرسلة، فإننا نعتبر هذا الوسيط حارسًا.

يتضح من ذلك أن السياسة الأمنية التي يطبقها «الحارس» تكون أكثر تعقيدًا مما يقوم به الوسيط، ولذلك فالبرامج التي يبرمج بها الحارس هي بدورها أكثر تعقيدًا، ومن ثم فهذه البرامج أكثر عرضة للخطأ، ويعتبر هذا أحد عيوب الحارس. وهناك «جدران حماية» أخرى تتفاوت في درجة البساطة ودرجة التعرض للخطأ.

١١ . ٦ مقارنة أنواع جدران الحماية

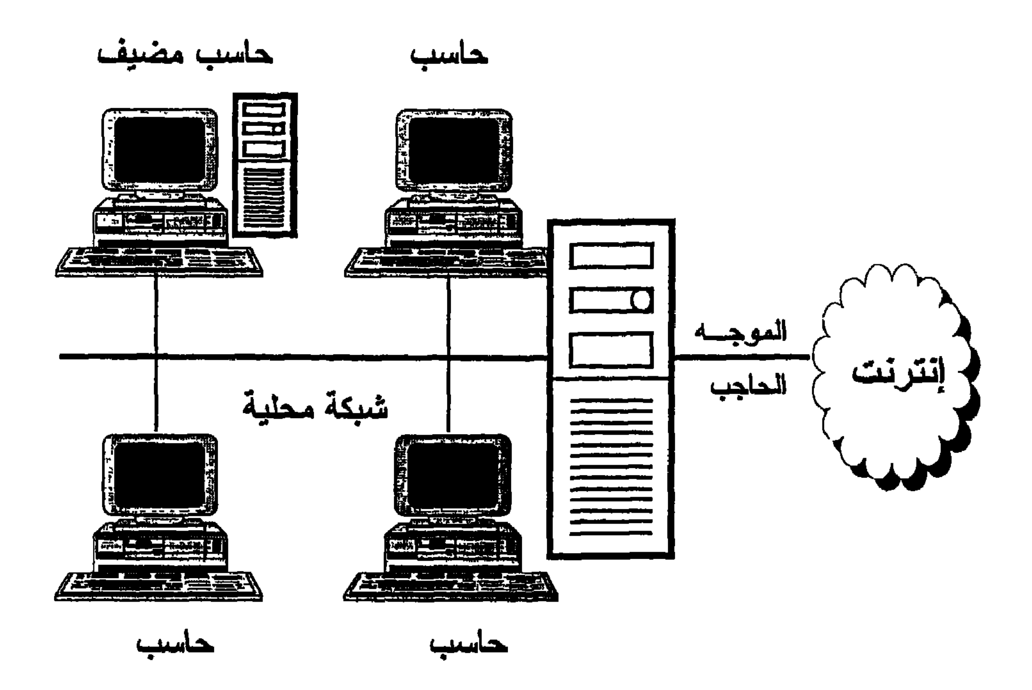
يبين الجدول (١١ ـ ١) مقارنة بين بعض أنواع جدران الحماية:

الموجه الحاجب	الوسيط	الحارس
الأكثر بساطة	معقد بعض الشيء.	أشدهم تعقيداً.
لا يرى سوى العناوين ونوع البروتوكول المستخدم	يرى النص الكامل للرسالة.	يرى النص الكامل للرسالة.
عملية الرقابة على الأنشطة صعبة.	يمكن مراقبة الأنشطة.	يمكن مراقبة الأنشطة.
قرار السماح أو المنع يعتمد على القواعد الموضوعة للاتصال.	قرار السماح أو المنع يعتمد على سلوك البرنامج المركب.	قرار السماح أو المنع يتوقف على تفسير محتويات الرسالة.
إذا كانت قواعد العنونة معقدة يمكن أن يصبح التركيب صعباً.	يمكن أن يكون البديل المناسب في حالة قواعد العنونة المعقدة.	الوظائف المعقدة للحارس تقلص من درجة الثقة به.

جدول (١١ ـ ١) مقارنة بين بعض أنواع جدران الحماية

١١ . ٧ أمثلة على بنية جدران الحماية

فيما يلي بعض الأمثلة التي نعرضها كمواقف ، هذه المواقف توضح كيف يمكن لجدار الحماية أن يحقق السياسة الأمنية للمنظمة ، ويبين الشكل (١١ - ٦) أبسط استخدامات جدار الحماية .



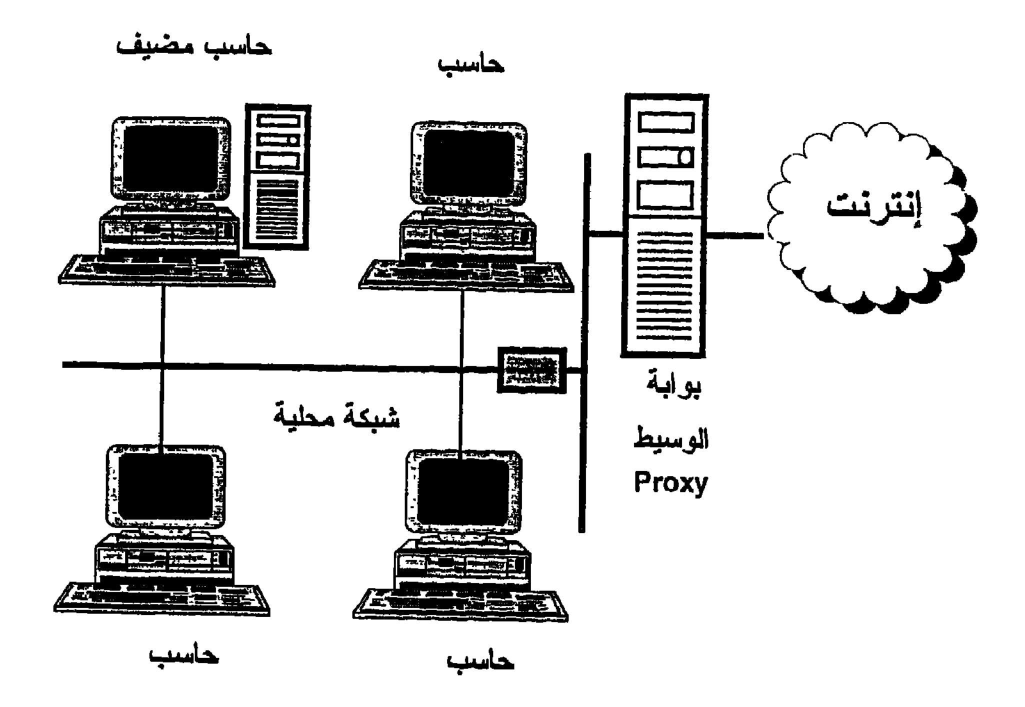
شكل (١١-٦) جدار حماية باستخدام الموجه الحاجب

١١ . ٧ . ١ جدار حماية باستخدام الموجه الحاجب

هذه البيئة تضم موجهًا حاجبًا موضوعًا بين الشبكة المحلية الداخلية والشبكة الخارجية، وهذا التصميم يكون كافيًا في كثير من الأحيان التي يكون فيها كل المطلوب من الموجه هو حجب بعض العناوين فقط، ولا يكون استخدام الوسيط في هذه الحالة اختيارًا موفقًا. وبالمثل فإن تركيب موجه يتولى فحص مجموعة ضخمة من العناوين لتحديد قبول الرسائل الواردة منها أو رفضها فالموجه أيضًا اختيار غير موفق.

١١ . ٧ . ٢ جدار حماية مركب على شبكة مستقلة

أما الأمر الذي يقلق خبراء أمن البيانات باستمرار هو أنه إذا أمكن اختراق جدار الحماية الموجه بنجاح فإن كل البيانات المتبادلة على الشبكة الداخلية المركب عليها جدار الحماية هذا يمكن (رؤيتها)، ولكي نعالج هذا الأمر يتم عادة تركيب حائط نار من نوع الوسيط على الشبكة الداخلية كما يبين الشكل (١١ - ٧). وبهذه الطريقة فإن البيانات التي يمكن رؤيتها على الشبكة المحلية في حالة اختراق جدار الحماية هي فقط تلك البيانات المتجهة إلى جدار الحماية أو الواردة منه وليست البيانات الموجودة على الشبكة الداخلية.



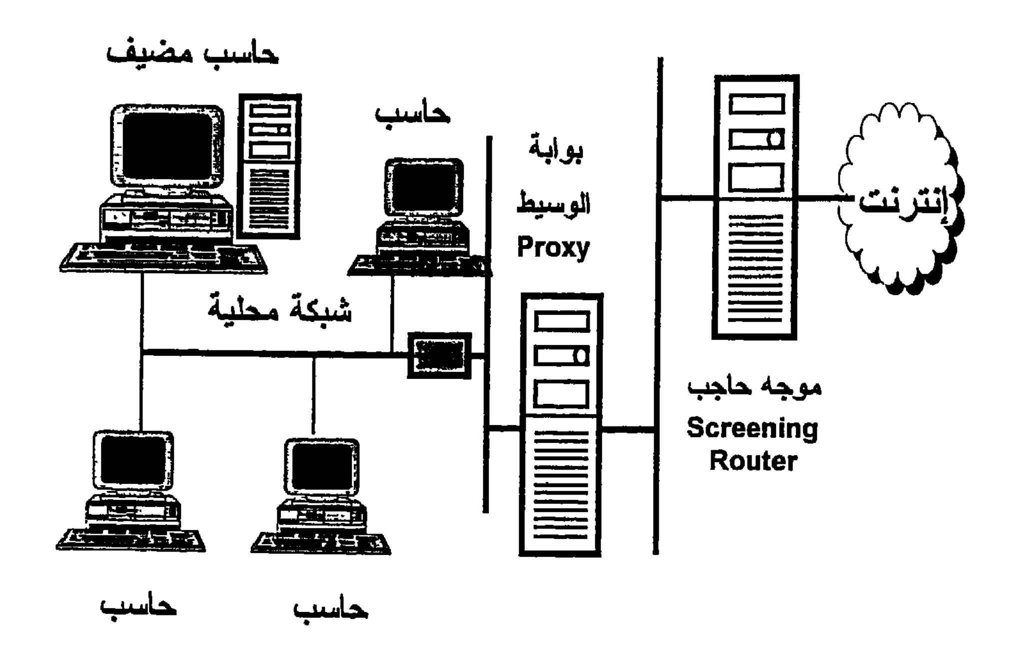
شكل (١١-٧) جدار الحماية مركب على شبكة مستقلة

شكل (١١-٧) جدار الحماية مركب على شبكة مستقلة

١١ . ٧ . ٣ جدار حماية باستخدام موجه ووسيط معًا

ومن أجل توفير حماية أفضل يمكن أن نضيف موجهًا حاجبًا لهذه المجموعة كما يبين الشكل (١١ – ٨)، وفي هذه الحالة يتولى الموجه الحاجب مهمة التأكد من صحة العناوين نيابة عن جدار الحماية الوسيط (وبذلك لا يمكن خداع جدار الحماية الوسيط عن طريق مهاجم من الخارج يدعي لنفسه عنوانًا من الداخل)، بينما يقوم جدار الحماية الوسيط بتصفية البريد الوارد

وفقًا لقواعده الخاصة المبرمج على أساسها، فإذا أمكن اختراق الموجه الحاجب فإن البريد الوارد إلى الوسيط وحده هو الذي سيكون معرضًا للاطلاع وليس أي من المعلومات الحساسة على الشبكة الداخلية .



شكل (١١ ـ ٨) جدار الحماية باستخدام وسيط وموجه معاً

الفصل الثاني عشر
الأمن والتقنية

١٢ . ١ التقنية في صناعة الأمن .

١٢ . ٢ استخدام التقنية في الجريمة .

الأمن والتقنية

خصصنا هذا الفصل للتقنية ودورها في صناعة الأمن (سلبًا وإيجابًا)، فنبدأ بالجانب الإيجابي فنوضح كيف استفادت صناعة الأمن بصفة عامة وأمن المعلومات بصفة خاصة من تطور التقنية، فنتحدث عن كيف يتم التفتيش الذاتي في المطارات عن بعد، وكيف يمكن اكتشاف الطرود المفخخة في مكاتب البريد، وكيف يمكن اكتشاف المتطفلين بزرع وسائل استشعار في باطن الأرض، أو إحاطة المنطقة بأسوار أشعة الليزر، أو استخدام التصوير الحراري. وكيف يمكن تحديد الهوية باستخدام البطاقات الذكية، ووسائل إعاقة السيارات الانتحارية، واستخدام التصوير التليفزيوني المتحرك لمقاومة الغرباء المتسللين واكتشاف أماكن اختبائهم. كما نتحدث عن تقنيات تأمين الاتصالات اللاسلكية ومكافحة التنصت الإلكتروني والتجسس الصناعي، ونتحدث عن بعض الشركات التي تتولى إعداد نظم أمنية متكاملة وتسلمها كاملة (تسليم مفتاح)، وكيف يعد الحاسب الآلي سيناريو اختبار إجراءات الأمن لتقييمها. ثم نتحدث عن استخدام «الروبوت» في العمليات الخطيرة التي لا يستطيع الإنسان المخاطرة بالقيام بها.

وفي القسم الثاني من هذا الفصل نبرز الوجه الآخر للصورة، وهو كيف تستفيد الجريمة من التقنية، فنتحدث عن بعض التقنيات الحديثة مثل تقنية «الملفات المتدفقة»، وأسلوب «الاقتحام السلبي حيث يكمن المجرم في مكانه وينتظر إلى أن تأتي الضحية إليه طائعة مختارة، ونختتم بالحديث عن البرامج «الفاحصة» (Sniffers) وخطورتها البالغة على أمن المعلومات.

١٢ . ١ التقنية في صناعة الأمن

١٢ . ١ . ١ تفتيش ذاتي عن بعد !

وجدت المنجزات التقنية طريقها إلى الاستفادة منها في مجالات أخرى جديدة مثل دخول الركاب إلى صالات المطار، وفحص الحقائب، وتفتيش الركاب (عن طريق أجهزة الأشعة الخفية). فمثلاً قد تطورت أجهزة أشعة إكس بشكل ملحوظ، فقد قامت بعض الشركات مؤخرًا بإنتاج أجهزة تكشف بوضوح شديد الأسلحة المخبأة في الملابس أو المواد المخدرة التي قد تكون مخبأة في أحشاء المهرب. بل إن هناك جهاز جديد للأشعة يمكنه، عند تعريض المسافرين العابرين من بوابات المطار للأشعة الصادرة منه، عرض صورهم كما لو كانوا شبه متجردين من ملابسهم. ولا يزال الجدل يدور حول مشروعية هذه الأجهزة وما إذا كان ينبغي استخدامها أم لا.

١٢ . ١ . ٢ الطرود المفخخة لم تعد تسبب قلقًا

في مكاتب البريد هناك ضرورة لفحص البريد الوارد خوفًا من الطرود المفخخة، وتستخدم الآن في ذلك أجهزة أشعة إكس من النوع الصغير مثل تلك التي تنتجها شركة «جراسبي سكيوريتي» (Graseby Security). وقد أدت هذه الأجهزة إلى الحد بشكل كبير من حوادث انفجار الطرود في مكاتب البريد، كما تنتج الشركة نفسها جهازًا لاكتشاف المتفجرات يمَكِّن مسئولي الأمن من اختبار الحقائب اليدوية الخاصة بمرتادي الأسواق ودور السينما، أو اللفافات المريبة التي قد توجد مهملة في الأسواق أو محطات الأتوبيس والتي يُخشى من أن تحتوي على قنابل صغيرة. وهذا مثال على الهدايا التي تقدمها تقنيات أمن المطارات للمجالات الأمنية الأخرى، فقد

انتقلت التقنيات المتقدمة المستخدمة في فحص ركاب الطائرات بالأشعة إلى المكاتب ومباني السجون وغيرها من المواقع المعرضة للأخطار.

١٢ . ١ .٣ كابلات مدفونة في الأرض تكتشف المتطفلين

درجة احتمال حدوث الخطر ومدى حساسية الموقع هي التي تفرض درجة الحماية المطلوبة التي قد تكون مجرد سلسلة حديدية ضخمة على الباب، أو سور من الأسلاك الشائكة، أو ربما سور مكهرب. وقد يتطلب الأمر في بعض الأحيان الجمع بين هذه الاستحكامات كلها، بل وربما الاستعانة ببعض وسائل الاستشعار الخفية مثل الأشعة تحت الحمراء أو الكابلات الحساسة للاهتزازات التي يتم دفنها في باطن الأرض. وقد ظهر حديثًا نظام جديد يستخدم كابلات محورية مدفونة في الأرض، فتقوم هذه الكابلات ببث موجات محدودة الطاقة على ترددات الراديو ثم تعيد استقبال هذه الموجات مرة أخرى، فإذا حدث أي تغير في الوسط المحيط نتيجة وجود جسم غريب في المنطقة المراقبة تتغير هذه الموجات عند إعادة استقبالها ومن ثم تنطلق أجراس الإنذار في غرفة المراقبة معلنة عن وجود متطفلين.

١٢ . ١ . ٤ أسوار أشعة الليزر

أسوار أشعة الليزر هي وسيلة أخرى لتأمين المناطق المكشوفة ضد الاقتحام، فنظام «سولاريس» الذي أنتجته شركة «إنتلسك آند شورتس» يحتوي على عدد من وحدات إطلاق أشعة الليزر يتم تركيبها على مسافات تصل إلى كيلومتر واحد، وتحتوي كل وحدة على معالج إلكتروني ودائرة خاصة للاتصال بنقطة تحكم مركزية. وعند تسلل شخص ما إلى المنطقة وقطعه لخطوط أشعة الليزر يقوم المعالج الإلكتروني بتوليد إشارة مناسبة يتم نقلها إلى غرفة التحكم بواسطة دائرة الاتصال.

وغني عن الذكر أنه أيًا كان النظام المستخدم من بين النظم المذكورة فإن نجاح هذا النظام يتوقف إلى حد كبير على كفاءة وتدريب رجال الأمن المكلفين بتنفيذه ويقظتهم المستمرة وحماسهم الدائم.

١٢ . ١ . ٥ التصوير الحراري يكتشف الغرباء

في المواقع الهامة من الشائع استخدام الدوائر التليفزيونية المغلقة، ولكن الجديد أنه يتم الآن دعم هذه النظم بواسطة أجهزة التصوير الحرارية التي يمكنها تصوير الأجسام عن طريق التعرف على الحرارة الصادرة منها، ويتم نقل الصور الملتقطة إلى غرفة التحكم المركزية، فإذا انطلقت صفارات الإنذار نتيجة اقتحام شخص غريب فإن مسئولي الأمن بالغرفة يمكنهم التأكد من هوية الداخل من خلال الصور التليفزيونية أو الحرارية قبل تحديد رد الفعل اللازم. وكثيرًا ما يتم تدعيم شبكة الكاميرات التليفزيونية الخارجية بعدة كاميرات داخلية إضافية موزعة على ممرات وغرف المبنى من الداخل لإحكام الرقابة من ناحية ومتابعة المقتحم من ناحية أخرى.

أما نظم «آجيما» (Agema) للأشعة تحت الحمراء فإن الطلب يزداد عليها بسبب جهاز التصوير الحراري الذي يخضع صور الأهداف، التي يتم اكتشافها عن طريق الأشعة تحت الحمراء، للمعالجة الرقمية بهدف إنتاج صور واضحة حتى في الأحوال الجوية السيئة.

١٢ . ١ . ٦ بصمات الأصابع وقاع العين .. ثم البطاقات الذكية

من النظم التي فتح التطور التقني الباب لها استخدام بصمات الأصابع أو بصمة قاع العين كوسائل لتحديد الشخصية، وهذه الوسائل يكون اقتناؤها له ما يبرره في حالة مراقبة الدخول إلى الأماكن ذات الحساسية الأمنية العالية أو الأماكن التي تكون درجة تعرضها لخطر الاقتحام كبيرة.

ولكن عندما تكون أعداد الموظفين المصرح لهم بالدخول إلى المبنى كبيرة فإن بطاقات «ويجاند» (Wiegand) الذكية تقدم الحل العملي، فالأسلاك الدقيقة المبثوثة في جسم البطاقة تقوم بمهمة تمييز شخصية حاملها وتسمح له بالدخول عند مروره بإحدى نقاط العبور. ولكن يبقى دائمًا عنصر (الرقابة المرئية) ضروريًا وهامًا لأي نظام أمني.

١٢ . ١ . ٧ مقاومة اقتحام السيارات!

بالنسبة للتحكم في دخول السيارات إلى المواقع الهامة فقد لاقت هذه المشكلة اهتمامًا كبيرًا من شركات المعدات الأمنية، خاصة بعد العديد من الحوادث الأمنية الأخيرة. ووسائل الإعاقة وأدوات إغلاق الطرق التي تنتجها بعض الشركات مثل شركة «إلكوستا سكيوريتي» (Elkosta Security) تتيح أساليب فعالة لإيقاف السيارات ومنعها من الدخول حتى لو كان يقودها شخص انتحاري!.

١٢ . ١ . ٨ الحائط الأمني

من المؤكد أن خطط تأمين المنشأة ووسائل هذا التأمين يجب أن تكون محاطة بالسرية، كما يجب ألا تكون بديهية حتى لا يتوقعها المجرم. ولذلك، ومن أجل حماية المباني من الداخل ضد خطر الاقتحام الإرهابي من خلال هجوم مباشر أعلنت شركة «بريتيش جيبسوم» البريطانية (British Gypsum) مؤخرًا عن نظام (الحائط الأمني(الذي يسمح بفترة من الحماية وتعطيل المهاجمين تصل إلى ٥١ دقيقة ضد هجوم متواصل تستخدم فيه أدوات مثل العتلات والمعاول والجواريف.

١٢ . ١ . ٩ سيارة للرقابة التليفزيونية المتحركة

بالنسبة للساحات الكبيرة مترامية الأطراف يصعب تركيب كاميرات بالأسوار على مسافات معقولة تتيح إحكام الرقابة. وفي مثل هذه الأحوال يمكن استخدام جهاز المراقبة المدمج من إنتاج شركة «نانو كويست» والذي يعتمد على الأشعة تحت الحمراء. هذا الجهاز يتم تركيبه على سيارة متحركة وتجوب هذه السيارة الأسوار في ورديات مستمرة، ويمكن استخدام أكثر من سيارة كلما اتسعت المساحة المطلوب تغطيتها.

١٢ . ١ . ١٠ المراقبة بالفيديو لاكتشاف الأهداف المتحركة (والساكنة)!

بعض نظم المراقبة بالفيديو تتضمن إمكانية اكتشاف أي أهداف متحركة، وبذلك يمكن تنبيه غرفة التحكم (بواسطة جرس إنذار) بمجرد أن يدخل المقتحم إلى مجال الرؤية الخاص بالكاميرا. وفي خطوة أكثر تقدمًا وتعد بتطورات أكبر في المستقبل قامت مؤخرًا شركة «أسترا دفيلوبمنتس» Astra Developments بإنتاج نظام يمكنه اكتشاف الأهداف غير المتحركة وذلك كوسيلة أمنية إضافية تناسب المناطق المزدحمة، حيث يمكن أن يكون أي هدف ساكن أو ربما شخص كامن بين الأشجار مثلاً مصدرًا للخطر.

١٢ . ١ . ١١ التسجيل بالفيديو لجمع الأدلة

من المهم في كثير من الأحيان أن يكون التسجيل بواسطة الفيديو جزءًا أساسيًا من أي نظام مراقبة، لأنه قد يكون من الضروري جمع الأدلة الخاصة بتحديد الهوية والأدلة التي تثبت ارتكاب المجرم لجريمته، ولذلك يجب أن يتم التسجيل قبل وبعد الحادث. وكانت هذه الحقيقة وراء النظام الجديد الذي أنتجته شركة «إي دي إس» (EDS) للإلكترونيات، وهو نظام تسجيل

الصورة اللحظي (IRIS) أو (Instance Recording Image System)، ويتيح هذا النظام عملية استرجاع الصور بسهولة لأن كل صورة تأخذ رقمًا رمزيًا مرتبطًا بتوقيت التقاطها، ويطلق عليه (Time Code Number)، ويمكن الاحتفاظ بهذه الصور بتخزينها إلكترونيًا مما يتيح عرضها على شاشة المراقبة بدرجة عالية من الدقة والوضوح.

١٢ . ١ . ١٢ تأمين الاتصالات اللاسلكية

يعتبر الاتصال اللاسلكي عنصرًا أساسيًا في أي نظام مراقبة أمنية، وما من شك في أن المجرمين المحترفين أو الإرهابيين المدربين لديهم الوسائل التي تمكنهم من مراقبة الموجات اللاسلكية للشرطة، ولذلك أصبح من الضروري تزويد دوريات الشرطة بأجهزة لاسلكية مؤمنة الاتصالات. ولقى جهاز «كوجارنت» (Cougarnet) الذي أنتجته شركة «راكال راديو» رواجًا في عدد كبير من الدول، وهذا الجهاز هو واحد من عدة نظم اتصالات لاسلكية مؤمنة متاحة حاليًا في الأسواق يعتمد معظمها على تشفير المكالمات قبل بثها حتى لا يستطيع من يلتقطها الاستفادة منها.

١٢ . ١ . ١٣ التنصت الإلكتروني والتجسس الصناعي

أصبحت أجهزة التنصت الإلكترونية مألوفة للغاية هذه الأيام، وهي الأجهزة المستخدمة لاستراق السمع بدءًا من اختراق خطوط الهاتف، ووصولاً إلى الدخول غير المشروع إلى أجهزة الحاسب الآلي بهدف سرقة المعلومات المخزنة فيه. والتجسس الصناعي الآن أصبح منتشرًا بشكل كبير على مستوى الدول وعلى مستوى الشركات المتنافسة. ولكن من الممكن حماية هذه المعلومات باستخدام وسائل المكافحة المناسبة، وبمراقبة الأماكن

الأكثر عرضة للتنصت، مثل غرف اجتماعات مجلس الإدارة بالشركات، أو غيرها من الأماكن التي تتم فيها الاجتماعات السياسية أو الفنية. مثل هذه الأماكن تحتاج إلى فحصها بشكل دوري للتأكد من عدم وجود أدوات تنصت مخفية.

١٢ . ١ . ١٤ نظم أمنية تسليم مفتاح!

تقدم شركة «بل سكيوريتي» (Bell Security) خدمة الفحص الأمني الإلكتروني ضمن خدماتها التي تقدمها جاهزة متكاملة أو بنظام (تسليم المفتاح) للبنوك، والمكاتب التجارية، والمباني الدبلوماسية، ومقار السفارات الأجنبية، وغيرها. وبرغم أن هذه الشركة لا تقوم بصناعة المعدات الأمنية إلا أنها تتولى اختيار وتجميع المعدات الأمنية المختلفة وفقًا لما تتطلبه احتياجات الخدمة التي تتولى تقديمها. وتشمل هذه الخدمات مقاومة الاقتحام، وتوفير الأمن المادي للمنشآت بصفة عامة. ولما كانت دول الشرق الأوسط من الدول التي تُعرف بافتقارها إلى خبراء أمن الحاسب المدربين فقد مدت بعض شركات أمن المعلومات خدماتها في مجال تأمين الحاسب الآلي إلى هذه الدول وأنشأت وكالات تمثلها في بعض دول الخليج مثل عمان ودولة الإمارات العربية والكويت.

١٢ . ١ . ١٥ الحاسب يؤلف السيناريو!

إذا كان الهجوم المتوقع هجومًا ضخمًا تستخدم فيه أسلحة مثل السيارات الملغومة لاقتحام المبنى، فهناك عدد من الوسائل التي تستخدم الحاسب الآلي لإعداد وتجربة برامج افتراضية من قبيل (ماذا لو ؟). وتبين هذه البرامج مناطق الضعف أو التعرض في المبنى بحيث يمكن تطبيق أسلوب

لحماية المناسب في كل حالة. ومن خلال هذه البرامج يستطيع رجال الأمن التخطيط لمختلف السيناريوهات المتوقعة ويقدمون النصيحة الملائمة حول أفضل طرق الإخلاء مثلاً وأكثرها أمنًا في حالة حدوث الكارثة.

وهناك شركات أمنية كبيرة مثل «فريزر ناش» للاستشارات، و«رويال أوردنيس» للخدمات الأمنية، و«كامبريدج» للاستشارات، و«دبليو إس إتكنز». هذه الشركات هي من بين الشركات ذات الخبرة الطويلة في تقييم درجة تعرض المواقع ومدى ضعفها في مواجهة خطر اقتحام الإرهابيين.

١٢ . ١ . ١٦ استخدام الروبوت في العمليات الخطرة

يُستخدم الآن الإنسان الآلي (أو الروبوت) في مختلف أغراض الأمن بدءًا من القيام بدور حارس الأمن المدرب، ووصولاً إلى فحص الأغراض المشتبه فيها للتأكد من خلوها من المتفجرات، مرورًا بعمليات اقتحام المناطق المشتعلة في الحرائق. وفي هذا المجال أعلنت شركة «جيات» (Giat) عن إنتاجها للروبوت الجديد المتخصص في فحص الأغراض المشتبه فيها، وتفكيك المتفجرات في حال وجودها. وهذا الروبوت يمكن استخدامه في المناطق التي تشكل خطرًا على دخول الإنسان إليها مثل حقول الألغام.

١٢ . ٢ استخدام التقنية في الجريمة

١٢ . ٢ . ١ تقنية «الملفات المتدفقة»

ظهرت في الأسواق مؤخرًا تقنية جديدة تسمى تقنية «الملفات المتدفقة» (Streaming Files) والخاصة بملفات الوسائط المتعددة، وهي ملفات إما صوتية أو فيدوية. وتضم هذه الملفات قطعاً من الموسيقى أو أفلام الفيديو

والتي تعرض على شاشة المستفيد في نفس الوقت الذي تبث به إلى الحاسب عبر شبكة الإنترنت. أما قبل استخدام هذه التقنية فكان على من يرغب في سماع مقطوعة موسيقية أو أو مشاهدة فيلم من أفلام الفيديو أن ينسخ الملف الذي يحتوي هذه المادة إلى القرص الصلب للحاسب الشخصي الخاص به بالكامل، قبل أن يستطيع سماعه أو مشاهدته. ومن المعروف أن ملفات الوسائط المتعددة (الصوت والفيديو) تتميز بكبر حجمها بالمقارنة مع ملفات النصوص، أو حتى ملفات الصور، وبالتالي فتحت هذه التقنية الباب أمام مروجي الأفلام الإباحية لبدء ما يُطلق عليه «ما يطلبه المشاهدون» بحيث يستطيع المستفيد الدخول إلى موقع معين ويطلب مشاهدة الفيلم المطلوب فيتم بثه مباشرة إلى جهازه. وبهذا يمكن مشاهدة أفلام طويلة لم يكن متاحًا مشاهدتها من قبل بسبب الحجم الهائل الذي تحتاجه على القرص الصلب الخاص بالمستفيد.

١٢ . ٢ . ٢ الاقتحام السلبي

من مفارقات التقنية، أو قل من أضرار التقنية، أن البرامج القوية الحديثة المستخدمة حاليًا لاستعراض المواقع، مثل تلك التي تستخدم برامج من نوع (Java applets) أو (Active X)، تتيح للمقتحمين الذين ينتوون مهاجمة المواقع أن يجلسوا وينتظروا الضحية حتى يأتي طائعًا إلى مواقعهم. ففي كل مرة تزور فيها موقعًا يمكن أن يكون لهذه الزيارة عواقب وخيمة، فموقع المجرم يمكن مثلاً أن يرسل إليك هدية غير مرغوب فيها من برامج «جافا» (applet) ليتم تنفيذها على حاسبك الشخصي. هذه الهدايا يمكن أن تمر حتى من خلال جدران الحماية التي تبدو آمنة حصينة. وفي لحظة ما إذا كنت تستخدم برنامج البريد الإلكتروني من «نت سكيب»، فإن هذا البرنامج الدخيل يمكنه الحصول على بريدك الإلكتروني وأن يرسل معلومات عن

شبكتك الداخلية من قبيل: عنوان الشبكة، واسم الحاسب المضيف في هذه الشبكة، ورقم المستفيد (User Id)، وكلمة المرور المشفرة. ثم يرسل كل هذه المعلومات إلى موقع المقتحم لاستخدامها في هجومه القادم.

أحيانًا قد يغريك موقع المقتحم بإنشاء رقم مستفيد خاص بك وكلمة مرور سرية، واعدًا إياك بالحصول على خدمات مغرية من هذا الموقع، دافعًا إياك إلى أن تقدم إلى المقتحم على طبق من فضة رقم المستفيد وكلمة المرور التي تستخدمها في مواقع أخرى للحصول على خدمات أخرى، أو ربما كنت تستعملها أيضًا على شبكتك الداخلية. فأنت طبعًا لا تريد أن يكون لديك العديد من أرقام المستفيد وكلمات المرور وتود توحيدها، وهنا تقع في الفخ المنصوب بمهارة فتكشف الاسم وكلمة المرور بلا جهد من جانب المقتحم. وهذه طريقة قديمة سهلة لم يعد الكثيرون من المستفيدين يقعون في حبائلها.

قد يسبب البرنامج الدخيل (applet) إيقاف حاسبك الشخصي عن العمل، ولكنه يبقى مع ذلك مختفيًا في جهازك، وعند إعادة تشغيل الجهاز مرة أخرى يعيد توصيلك بموقع المقتحم ليلتقط نسخة أخرى من البرنامج الدخيل لتقوم بإيقاف حاسبك عن العمل مرة ثانية، وهكذا.

ويستطيع البرنامج الدخيل كذلك تعديل البرنامج المستعرض (Browser) الذي تستخدمه ليعمل نيابة عن موقع المقتحم ويدمر المواقع الأخرى عندما تقوم أنت بزيارتها. أي أنه يجعل منك مقتحمًا دون أن تدري (شيء مثل أسطورة مصاص الدماء «دراكيولا» الذي يحول ضحاياه ممن امتص دماءهم إلى مصاصي دماء جدد!).

الوسيلة البديهية لمجابهة هذه المشاكل هي تجنب زيارة المواقع المشبوهة أو غير الموثوق بها. فإذا أنت غامرت بدخول مثل هذه الأدغال، فعلى الأقل

تأكد خلال هذه الرحلة من أن البرنامج المستعرض الذي تستخدمه لن ينفذ برامج «جافا» أو «آكتف إكس». وإذا كانت إحدى المؤسسات أو الشركات تستخدم «جدار الحماية» (Fire wall)، فيجب تهيئة جدار الحماية بحيث يمنع البرامج من هذا النوع وغيرها من الملفات المشكوك فيها، وكذلك يجب أن تمنع هذه الجهات دخول موظفيها إلى المواقع المشبوهة من خلال «الوسيط» (Proxy) أو «جدار الحماية»، فالتجول في المواقع يشبه التجول في الطرقات، فلا يجب أن تدخل إلى الأحياء أو المناطق التي قد يصيبك فيها ما لا ترضاه.

١٢ . ٢ . ٣ البرامج الفاحصة

البرامج «الفاحصة» (Sniffers) نقصد بها تلك البرامج التي تعمل في الخفاء وتفحص كل حزمة بيانات عند مرورها خلال شبكات حزم البيانات (Packet-switching networks) مثل شبكة الإنترنت. ويستخدم المقتحمون هذه البرامج الفاحصة للحصول على المعلومات التي يمكنهم استخدامها لتخريب الحاسب الخاص بالضحية تحقيقًا لأغراضهم غير المشروعة.

خلال الهجوم باستخدام البرامج الفاحصة فإن المعلومات المزمع إرسالها إلى أحد المواقع على شبكة الإنترنت تمر بالعديد من المواقع في العديد من الدول خلال رحلتها في هذه الشبكة الهائلة. وبعض هذه المواقع التي تمر بها المعلومات تكون بريئة ولكن بعضها قد يكون مواقع غير بريئة.

وتكمن البرام الفاحصة في بعض المواقع حيث تعمل سرًا، ويمكن تصورها وكأنها مواقع غير مرئية على الشبكة، تمامًا مثلما كان حصان طروادة مختفيًا ضمن برنامج آخر. وتقوم هذه البرامج بفحص كل حزمة بيانات تمر بحثًا عن المعلومات المطلوب الحصول عليها، مثل كلمات المرور للمستفيدين والتي يمكن الحصول عليها من الحزمة الأولى المرسلة من المستفيد

إلى الموقع عند إتمام عملية الدخول (Logon) إلى هذا الموقع، حيث أنه من الطبيعي أن تكون كلمة السر مطلوبة عند الدخول إلى الموقع. ويستطيع البرنامج الفاحص تمييز هذه الحزمة لأن كل هذه المعلومات موجودة في مقدمة الحزمة (ترتيب الحزمة في الرسالة، والجهة المرسلة إليها، والجهة المرسلة منها).

يعتقد كثير من خبراء أمن المعلومات أن شبكة الإنترنت تعاني حاليًا من شيوع استخدام هذه البرامج التي أصبحت كالوباء يجتاح الشبكة حيث يتم كشف وسرقة عشرات الألوف من كلمات المرور (Parker,1998). ومن المعتقد أن المجرمين سوف يتوسعون في المستقبل في استخدام مثل هذه البرامج لارتكاب المزيد والمزيد من الجرائم مما يُطلق عليه اسم «الجريمة الآلية» (Automated Crime).

الفصل الثالث عشر

وسائل الإعلام وجرائم المعلومات

١٣ . ١ الإعلام عصا سحرية .

١٣ . ٢ الوعي المعلوماتي .

١٣ . ٣ إخفاء الحقائق .

١٣ . ٤ التغطية الإعلامية .

١٣ . ٥ جرائم نظم المعلومات .

وسائل الإعلام وجرائم المعلومات

نخصص هذا الفصل لوسائل الإعلام، هذه الأداة الخطيرة المؤثرة في الجماهير، فنبدأ بتوضيح أثرها الفعلي، ثم نتحدث عن الوعي المعلوماتي لدى العامة، وأهميته. ثم نتطرق إلى قضية شائكة، وهي رفض الكثير من الحكومات أو الشركات أو المؤسسات الإفصاح عما تتعرض له من جرائم معلوماتية، أو عن حجم الخسائر التي تنجم عنها. وننتقل بعد ذلك إلى الحديث عن التغطية الإعلامية للحاسب الآلي وجرائم نظم المعلومات في وسائل الإعلام المختلفة من صحافة وسينما وتلفاز وغيرها من وسائل مرئية ومقروءة ومسموعة، وكيف يمكن أن تؤثر التغطية الإعلامية الخاطئة سلبًا على فهم العامة لقضايا أمن المعلومات. ثم نختتم الفصل بالدعوة إلى ضرورة مناقشة جرائم نظم المعلومات في المؤتمرات العلمية والفوائد التي يمكن أن نجنيها من ذلك.

١٣ . ١ الإعلام عصا سحرية

الإعلام هو العصا السحرية التي توجه الجماهير في معظم الدول سواء الدول المتقدمة أو النامية، فالإعلام بأدواته المختلفة المسموعة والمقروءة والمرئية يشكل في الوقت نفسه مصدرًا مهمًا من مصادر المعرفة لكثير من البشر. ولذلك فيجب الاستفادة من الإعلام في توعية مستخدمي الحاسب الآلي في شتى المجالات، خاصة بعد انتشار ذلك الأخير في كل مجال.

في الوقت نفسه يجب أن يتصدى لهذه التوعية متخصصون بأمل أن تحدث كلماتهم الأثر المطلوب، وألا يقعوا في فخ المبالغة والتهويل، أو في فخ الإثارة، أو في فخ التبسيط المخل بالموضوعات المطروحة. وتحتوي برامج التلفاز والإذاعة على الكثير من البرامج العالمية المنتجة في الدول المتقدمة والتي

تبسط الحقائق العلمية والمعلومات المهمة للجمهور العادي، فضلاً عن تقديم المعلومات عن أحدث المستجدات للمتخصصين في مجال الحاسب.

ولعلنا نلمس بوضوح كيف أن وسائل الإعلام أثبتت أنها فعالة ومؤثرة في رفع درجة الوعي الأمني لدى الكافة وفي حفز الأفراد على حماية معلوماتهم المخزنة في الحاسبات.

١٣ . ٢ الوعي المعلوماتي

فرضت المعلوماتية مشكلات استدعت تدخلات عاجلة مدروسة من جهات التشريع ومن رجال القانون لتحقيق التوازن بين حقوق المبدعين ومن يجاورهم من جانب، وحقوق المتلقين ومستخدمي هذا الإبداع من جانب آخر في عالم تلاشت فيه الحدود ويتم فيه تداول المعلومات بكل صورها وأشكالها بسهولة ويسر وبغير قيود. هذه المتغيرات جميعها تتطلب دعم (الوعي المعلوماتي) لدي العامة بهدف تحقيق هذا التوازن بين الحق المترتب للمبدعين في مقابل جهدهم وبين الحق في المعرفة، وهو توازن صعب المنال في إطار ثورة الاتصالات الحالية التي لا تكف كل يوم عن أن تقدم لنا الدليل علي عجز الإنسان عن ملاحقتها~، خاصة أن هناك منافسة شرسة بين دول العالم في سرعة الاستفادة من نتائج تطور التقنية وإذا ما كانت الدول المتقدمة تعي الآثار السلبية للتقنيات الحديثة للمعلومات وترشد من استخدامها بين الجماهير~، إلا أن العديد من الدول النامية والتي مازالت تعاني من مشاكل الأمية والتخلف العلمي والتقني تواجه مشاكل الآثار السلبية لنقل العديد من التقنيات الحديثة في مجال المعلومات منها تهديد تراثها الثقافي وقيمها الأخلاقية إلي جانب المخاطر الصحية التي تحيط بالجماهير نتيجة الاستخدام غير المرشد وغير الواعي لهذه التقنيات (Lutfy,1999).

١٣ . ٣ إخفاء الحقائق

الجريمة في مجال الأعمال كانت لها دائمًا علاقة بالمعلومات، والآن أصبحت لها، وبشكل متزايد، علاقة بالكمبيوتر كأداة للوصول إلى هذه المعلومات. وللأسف فمعلومات أصحاب الأعمال عن جرائم الحاسب يستقونها من تقارير وسائل الإعلام، ربما لأنها واسعة الانتشار أو لأنها قد تفرض نفسها عليهم دون أن يسعوا للحصول عليها.

ووسائل الإعلام بدورها لا تنشر كل الجرائم بل تنشر المثيرة منها فقط مثل أنباء المغامرين الذين يقتحمون شبكة وزارة الدفاع الأمريكية، أو أخبار الفيروسات (القاتلة!)، وهذه كلها من الجرائم نادرة الحدوث.

ووسائل الإعلام لا تنشر كل المعلومات عن كيفية ارتكاب الجريمة أو الدروس المستفادة منها، ولا تنشر كيفية تفادي وقوع مثل هذه الجرائم في المستقبل، ومن ثم فيالها من وسيلة قاصرة للتعلم.

في الواقع لا توجد إحصاءات دقيقة يعتمد عليها عن جرائم نظم المعلومات ومعدلات حدوثها أو حجم الخسائر فيها، ومن المؤسف أن معظم الاستبيانات القليلة التي أجريت على هذا النوع من الجرائم قد أجريت من قبل أشخاص لا يعلمون الكثير عن الحاسب وتكنولوجيا المعلومات، ومما زاد الأمر سوءًا أن كل شخص ممن استجابوا لهذه الاستبيانات كان لديه مفهوم مختلف عن جريمة نظم المعلومات، بل ربما كان بعضهم غير مدرك لطبيعة الجريمة التي يتحدث عنها أو كيفية ارتكابها أو حجم الخسارة الحقيقية فيها.

والاستفتاءات والاستبيانات والتحقيقات الصحفية التي تجرى على ضحايا مثل هذه الحوادث هي أيضًا مضللة لأن المؤسسات التي تقع ضحية

لهذه الأعمال الإجرامية عادة ما تفضل إخفاء حجم خسائرها وظروف حدوث هذه الخسائر اتقاء للحرج وإخفاء للثغرات التي قد توجد في نظامها الأمني. نتيجة لذلك فإن الحالات الهامة والتفاصيل المفيدة لا يطلع عليها الآخرون (الضحايا المحتملون)، اللَّهُمَّ إلا من خلال الأحاديث الجانبية ومراسلات البريد الإلكتروني غير الرسمية التي يتبادلها خبراء أمن المعلومات فيما بينهم ويتحدثون فيها (بحرية) عن تجاربهم وتجارب مؤسساتهم. هذا النقص الشديد في المعلومات الدقيقة المنشورة يؤثر بالفعل على نظرتنا لجرائم نظم المعلومات وحجمها وطبيعتها وطرق مقاومتها، فنراها إما بالكثير من التهويل أو بالكثير من التهوين!!.

١٣ . ٤ التغطية الإعلامية.

برغم أن معظم المعلومات التي حصل عليها جاسوس المخابرات المركزية الأمريكية(CIA) «ألدريخ آميس» (Aldrich Ames) ونقلها إلى الاتحاد السوفيتي كانت في صورة ورقية، إلا إن الصحافة قد صنفت أعماله باعتبارها جرائم كمبيوتر ذلك لأنه قام بإدخال هذه المعلومات المسروقة في حاسبه الشخصي ونقلها للسوفييت على أقراص مرنة.

وفي حادث مماثل أدى التحذير الذي أطلقه مكتب التحقيقات الفيدرالي الأمريكي (FBI) عن التجسس الاقتصادي الذي يتم بتمويل أجنبي، أدى إلى أن يعتقد الكثير من الناس أن التجسس يتم عن طريق اختراق الحاسبات الآلية، ولكن وفقًا لمصادر مكتب التحقيقات الفيدرالي فإن التجسس يتم في معظم الأحوال عن طريق الرشوة أو الخداع أو استمالة الموظفين ذوي المهام الحساسة، وأكد تقرير المكتب أن معظم المعلومات المسروقة تم الحصول عليها من البشر وليس من الكمبيوتر.

وبازدياد خبرة الصحفيين بالحاسب الآلي أصبحت التغطية الإعلامية لجرائم الحاسب أفضل من ذي قبل، فنرى صحفيين كادوا يتخصصون في هذه الموضوعات مثل «جون ماركوف» في جريدة «نيويورك تايمز» و «لو دولينار» في جريدة «يو إس توداي» و «جوشوا كيتنر» في مجلة «تايم» أو الصحفي الحر «جوناثان ليتمان» وفي عالمنا العربي نجد الصحفي «نديم عبده» في مجلة الكمبيوتر والإلكترونيات.

ونتمنى أن يزحف هذا الوعي إلى مجال السينما، إذ أن صورة الكمبيوتر في الأفلام السينمائية هي لا تتعدى جهازًا به العديد من المصابيح التي تومض بسرعة وتصدر ضوضاء غريبة، وأشرطة تدور وأزيز مستمر ينبئ عن أن هناك عمليات بحث تجرى أو معادلات رياضية عويصة يتم حلها، وهذا جميعه لا يستغرق سوى بضع ثوان مهما كانت درجة تعقيد العملية. وعادة ما تستطيع هذه الآلة أن تقوم بتنبؤات مستقبلية خارقة على شاشة السينما، ولقد رأينا هذه الصورة الغريبة للحاسب الآلي في بعض الأفلام الشهيرة مثل فيلم « المقتحمون» وفيلم «حدائق الديناصورات» وربما كان هذا الأخير يصلح فيلمًا تدريبيًا على أمن الحاسبات أكثر منه فيلمًا عن الحيوانات المنقرضة لكثرة ما يظهره من ثغرات أمنية فادحة بدءًا من ترك بقايا الطعام والشراب فوق أجهزة الحاسب إلى ذلك المبرمج الذي وضع البرنامج (بمفرده) ويقوم (بمفرده أيضًا) بتشغيل كمبيوتر على هذه الدرجة من الأهمية والحساسية، إذ يتحكم في تفريخ مخلوقات خطيرة كالديناصورات، بالإضافة إلى عدم الاهتمام بإيجاد مصدر مستمر للتيار غير معرض للانقطاع.

ولعلنا لا نجاوز الحقيقة كثيرًا إذا قلنا أن لدينا في العالم العربي مراكز للحاسب الآلي تعاني من الاختراقات الأمنية أكثر مما تظهره مثل هذه

الأفلام، وأن درجة الوعي الأمني في هذه المراكز منخفضة إلى حد ينذر بالخطر ويوجب التنبيه والتحذير.

وتكونت لدى جمهور السينما بعض المعتقدات عن الحاسب الآلي استقاها من الأفلام التي يشاهدها، منها أن مستخدمي الكمبيوتر والمشغلين والمبرمجين يرتدون دائمًا معاطف بيضاء نظيفة تحمل شارة مميزة «بادج» ومجموعة من الأقلام في كل جيب من جيوب المعطف، ويحملون عادة في أيديهم لوحة صغيرة مثبت عليها بعض الأوراق، وهم عادة يعرفون على الفور كيف يستخدمون أي حاسب في العالم أو حتى تلك الحاسبات التي قد تأتي من عوالم أخرى!.

ومن معتقدات جمهور السينما كذلك أن كل شاشات الحاسب تعرض باستمرار رسومًا مجسمة متحركة وتعرض صور أشخاص حقيقيين يتحدثون من الماضي أو من المستقبل. كما يعتقدون أن جميع الحاسبات قادرة على فهم اللغة الإنجليزية البسيطة، فإذا كتب البطل على لوحة المفاتيح «أريد الاطلاع على كل الملفات السرية»، فإن الحاسب يعرض عليه في الحال كل الملفات السرية! كما يقنعنا المخرجون أن كل البيانات المشفرة يمكن فك شفرتها في لحظات بواسطة متخصصي الكمبيوتر، وأن كلمة المرور (السرية) يمكن تخمينها في محاولتين أو ثلاث.

كما أذهلني كيف يصدق الجمهور أن عمليات التنصت على أجهزة الحاسب باستخدام الهوائيات الموجهة عملية سهلة وبسيطة وتنجح دائمًا في الحصول على المعلومات المطلوبة بالضبط!.

كما أن السينما حققت نجاحات مذهلة في مجال الاتصالات حيث نجد أن كل البوابات الإلكترونية ومحطات القوى وحتى المفاعلات الذرية

بالإضافة إلى أجهزة الحاسب الأخرى حول العالم يمكن أن يتم توصيلها على الفور وبكل يسر وسهولة بجهاز الحاسب، سواء الجهاز الخاص بالشرير أو الجهاز الخاص بالبطل! .

وكتب الخيال العلمي تجنح إلى إضفاء صفات مبالغ فيها عن الكمبيوتر وعما (يستطيع) الكمبيوتر أن يفعله، وتفترض قدرات خيالية في الكمبيوتر، ربما تتحقق بالفعل في المستقبل، ولكنها تشوه تمامًا الصورة الحقيقية للكمبيوتر. ونصيحتي لكتاب الروايات العلمية والأفلام التي تتعرض لجرائم الحاسب أن يستعينوا بخبراء الحاسبات عند إعدادهم للسيناريو فهم بذلك سيحصلون على فائدة كبيرة تضفي قيمة على أعمالهم الأدبية أو الفنية .

١٣ . ٥ جرائم نظم المعلومات

أدي انتشار التعامل بالأساليب التكنولوجية الحديثة مثل الحاسب الآلي والإنترنت إلي ظهور العديد من الأساليب الإجرامية المستحدثة التي لم تكن معروفة من قبل والتي أصبحت تهدد مصالح المجتمع والأفراد وتحتاج إلي حماية قانونية .

ويزيد انتشار هذه الوسائل المعلوماتية الحديثة من فرص انتشار هذا النوع الجديد من الجرائم (جرائم نظم المعلومات)، وهي الجرائم التي تتصل بالمعلوماتية. وهذه الجرائم يمكن ارتكابها عن طريق أساليب إجرامية مستحدثة لم تكن معروفة من قبل كفيروس الحاسب الذي يستخدم في تدمير البرامج، أو أسلوب السحب الآلي من الرصيد ممن ليس له صفه شرعية، كذلك جرائم التجسس عن بعد وسرقة بيانات تتعلق بالأمن القومي. فضلاً عما يمكن حدوثه من مساس بحياة الأفراد الخاصة وانتهاكها، أو وقوع جرائم تمس الآداب عن طريق شبكة الإنترنت .

وقد أُقيمت في أغسطس ١٩٩٩ في مدينة القاهرة ندوة لمناقشة الجوانب الأخلاقية والقانونية والمجتمعية للمعلومات لمناقشة جرائم التكنولوجيا الحديثة وموقف المشرع المصري من تجريمها. والندوة تولت تنظيمها اللجنة الوطنية المصرية للتربية والثقافة والعلوم التابعة لهيئة اليونسكو. وأكدت الندوة على أن وجود علاقة بين انتشار استخدام نظم الحاسب الآلي وانتشار استخدام شبكة الإنترنت من ناحية وارتكاب بعض الجرائم الجديدة على المجتمعات العربية من ناحية أخرى هو نتيجة طبيعية للتطور التكنولوجي الحالي.

وضع جرائم نظم المعلومات على بساط البحث ومناقشة الأساليب الإجرامية المستحدثة في مثل هذه الندوات مطلوب بشدة لوضع حد للكثير من الجرائم التي تمس مصالح المجتمع والأفراد وتحتاج إلي حماية قانونية وتشريعات جديدة. ويزيد من أهمية طرح هذه المشاكل على بساط البحث في المؤتمرات والندواتالعلمية أن الكثير من المؤسسات كالبنوك والشركات الكبرى تستخدم الحاسب الآلي بكثرة، بل تكاد تستخدمه في كل عملياتها.

الفصل الرابع عشر
التشريع وتجريم جرائم نظم المعلومات

١٤ . ١ الفراغ التشريعي الحالي .

١٤ . ٢ اختلاف التشريعات بين الدول .

١٤ . ٣ تجريم جرائم نظم المعلومات في أوروبا .

١٤ . ٤ التشريع في الدول العربية .

١٤ . ٥ الضوابط الدينية .

التشريع وتجريم جرائم نظم المعلومات

خصصنا هذا الفصل لدراسة موقف التشريع من تجريم جرائم نظم المعلومات، فنبدأ الفصل بالحديث عن الفراغ التشريعي الحالي، ثم نتحدث عن اختلاف التشريعات بين الدول المختلفة، ونبين موقف الاتحاد الأوروبي والدول الأوروبية من جرائم نظم المعلومات وجهودها نحو التوصل إلى تشريع موحد في هذا المجال خاصة وأن المعلومات تنتقل بحرية بين دول الاتحاد الأوروبي. وننتقل بعد ذلك إلى دعوة الدول العربية إلى دراسة هذه التشريعات وإصدار القوانين اللازمة لتجريم هذا النوع من الجرائم. ونختتم الفصل بالحديث عن الضوابط الدينية في هذا المجال.

لكي نفي هذا الموضوع الهام حقه فيستلزم الأمر دراسة مستقلة تحصر التشريعات في دول العالم والدول العربية، ثم تستخلص منها مقترحًا بتشريع موحد يناسب البيئة العربية، ويخرج ذلك عن نطاق هذا الكتاب.

١٤ . ١ الفراغ التشريعي الحالي

تزوير بيانات الحاسب هي جريمة أداتها استخدام طرفية ومسرح الجريمة فيها هو الحاسب الآلي نفسه، تمامًا كجريمة القتل التي قد تكون أداتها سلاحًا ناريًا أو سكينًا. وهذه الجريمة (التزوير) تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها، إذ يُعرِّف القانون البريطاني التزوير بأنه «يعتبر الشخص مدانًا بالتزوير إذا اصطنع أداة زائفة بنية استخدامها، سواء بنفسه أو بواسطة آخرين، لإقناع شخص ما بقبول هذه الأداة باعتبارها أداة حقيقية، فيقبلها نتيجة لذلك للقيام، أو عدم القيام، بعمل ما ينتج عنه ضرر له أو لآخرين». هذه الأداة في مجال الحاسب قد تكون قرصًا ممغنطًا أو شريطًا أو

أي وسط لحفظ البيانات. بينما ينص القانون الاسكتلندي على «الدخول إلى برنامج أو بيانات مخزنة على الحاسب يعتبر غير مشروع إذاتم ذلك بغرض الحصول على معلومات من البرنامج أو البيانات أو الإضافة إلى البرنامج أو البيانات أو الحذف من أيٍّ منهما أو التعديل في أيٍّ منهما، بنية الحصول على ميزة لنفسه أو لغيره أو إلحاق الضرر بمصالح شخص آخر (Collier,1994).

في بعض الأحوال ينتج عما نسميه جرائم الحاسب أضرار كبيرة (اقتصادية في الغالب)، ولكن الجرائم في هذه الحالة لا تقع في دائرة التجريم من جانب القانون الجنائي. فجرائم الحاسب لها خصوصية تجعل التشريع يقف عاجزًا عن تكييفها قانونيًا أو إخضاعها لمواد القانون الجنائي، من هذه الخصوصية أن جرائم الحاسب لا تقع على أرض دولة معينة بحيث يختص قضاء هذه الدولة بالنظر فيها، فقد يقوم شخص ما جالس أمام جهاز الحاسب الشخصي في دولة ما باستخدام نظام الحاسب في دولة أخرى ويقوم إما بالحصول على المعلومات أو تدميرها أو تزويرها. هذه السهولة في عبور النشاط الإجرامي للحدود يجب أن تجعلنا ننظر بشكل مختلف إلى جرائم الحاسب.

ونود أن ننبه هنا إلى أن جرائم الحاسب هي جرائم من نوع فريد وتحتاج إلى تشريعات خاصة ووسائل مختلفة للإثبات بل وتحتاج إلى شرطة خاصة لمكافحتها تكون مدربة بشكل خاص على هذا النوع من الجرائم. فبعض التشريعات تتطلب، كي تجرم الفعل، أن يكون هناك اقتحام أما بالنسبة للمعلومات فكيف نعرِّف الاقتحام؟ هل تخمين كلمة السر واستخدامها في الدخول إلى قاعدة بيانات للحصول على معلومات يعتبر اقتحامًا، وهل يشترط أن يقوم الحاسب بتحذير المقتحم عند الدخول إلى البيانات بأن ذلك يضعه تحت طائلة القانون.

أعتقد أن هناك تعديلات كثيرة مطلوب إدخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن استخدام الحاسب الآلي في مجال المعلومات وعن ظهور شبكات المعلومات العالمية. وأعتقد أن هذا يمكن أن يكون نقطة بحث جديدة ندعو البحاثة للاهتمام بها.

١٤ . ٢ اختلاف التشريعات بين الدول

١٤ . ٢ . ١ مشكلة انتقال المعلومات بين الدول

بعض الدول التي تضع قيودًا على تداول المعلومات تطلب، في حالة انتقال هذه المعلومات إلى دولة أخرى، أن تلتزم هذه الدولة بنفس مستوى الحماية المفروض على هذه المعلومات، وربما كان هذا من حق الدولة ولكن امتداد القيود عبر الدول مع اختلاف قوانين الدول عن بعضها يسبب مشاكل كثيرة لرجال الأعمال الذين يحتاجون إلى تبادل المعلومات عبر العالم وخاصة بعد ظهور شبكة الإنترنت. وفي الحقيقة فإن ظهور الإنترنت أنشأ أمرًا واقعًا لا تستطيع الدول أن تفعل شيئًا في مواجهته. هذا الأمر الواقع هو صعوبة ملاحقة المعلومات. فأنت تستطيع التحكم في أنبوب ينقل الماء من مكان إلى آخر وأن تراقب ما ينقله هذا الأنبوب، ولكنك لا تستطيع بأي حال من الأحوال أن تراقب الطوفان إذا زحف وأغرق واجتاح (داود ٢٠٠٠).

ويكتسب اختلاف القوانين بين الدول بعدًا أهم عندما تختلف درجة الحماية بين الدول، فالقانون البريطاني مثلاً كل ما يفرضه على مستخدم المعلومة أن يسجل استخدامه لها ولا يشترط حصوله على ترخيص بذلك، بينما القانون الألماني يشترط حصول مستخدم المعلومة على تصريح بذلك. فالقانون البريطاني إذن يمنح درجة من الحماية أقل من تلك التي يمنحها القانون الألماني (Hoeren,1994).

جرم المشرع الفرنسي العديد من جرائم نظم المعلومات ومنها جريمة التوصل بطريق التحايل إلي نظام المعالجة الآلية للبيانات . وتشدد العقوبة إذا نتج عن هذا التوصل محو أو تعديل في المعلومات الموجودة في داخل النظام أو إيقاف هذا النظام عن العمل أو تعطيله ، وتكون العقوبة هي الحبس من شهرين إلي عامين وغرامة تتراوح بين ١٠ آلاف و ١٠٠ ألف فرنك .

ومن جرائم نظم المعلومات المنتشرة جريمة إتلاف البرامج ، والمقصود بجريمة إتلاف برامج ومعلومات الحاسب الآلي هو تدمير محتواها المنطقي أي المحتوي ذاته المسجل علي وسط ما أيًا كان نوعه ، وتقع الجريمة إذا تم محو هذه المعلومات كليًا أو تم تشويه المعلومة أو البرنامج علي نحو يجعلها غير صالحه للاستعمال .

والسؤال الذي يطرح نفسه هو «هل يمثل هذا الإتلاف العمدي الصادر من الجاني إتلافا بالمعني المقصود في النص الجنائي أم لا؟» أي هل ينطبق عليه نص المادة ١/ ٦٣١ من قانون العقوبات المصري والتي تعاقب كل من ضرب أو أتلف عمدًا أموالاً ثابتة أو منقولة أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة؟

وكذلك بنفس المفهوم نص قانون العقوبات الفرنسي في المادة ٤٣٤ والتي تقرر العقاب علي كل من ضرب أو أتلف أموالا ثابتة أو منقولة مملوكة للغير .

فهل تنطبق هذه النصوص علي فعل أو تدمير أو إتلاف المال المعلوماتي المعنوي أم لا؟ للأسف فإن نص المادة ١/ ٣٦١ من قانون العقوبات المصري أو نص المادة ٤٣٤ من قانون العقوبات الفرنسي كلاهما لا ينص علي كون المال المعلوماتي المعنوي داخلاً في نطاق الأموال المنصوص عليها في تلك المواد .

وبالتالي : لتقرير الحماية يجب أولا التسليم بأن المال المعلوماتي المعنوي هو علي قدم المساواة في الحماية الجنائية مع الأموال التقليدية المنصوص عليها في هذه المواد، ثم ثانيا الاعتراف بإمكانية إتلافه وتقرير نفس العقوبة علي ارتكاب الإتلاف.

١٤ . ٣ تجريم جرائم نظم المعلومات في أوروبا.

١٤ . ٣ . ١ قائمة المجلس الأوروبي

اقترح المجلس الأوروبي على الدول الأعضاء فيه أن تلتزم بتعديل تشريعاتها الجنائية لتتضمن عدة جرائم من جرائم نظم المعلومات. وتضم هذه الأنشطة قائمة إجبارية وأخرى اختيارية. أما القائمة الإجبارية فتشمل :

- الاحتيال باستخدام الحاسب.
- التزوير باستخدام الحاسب.
- تدمير بيانات أو برامج الحاسب.
- تخريب الحاسب.
- الوصول للبيانات بدون تصريح.
- اعتراض مسار البيانات المنقولة بدون تصريح,
- إعادة إنتاج برامج الحاسب المحمية بدون تصريح.
- إعادة إنتاج الخرائط والرسوم بدون تصريح.

كما اقترح المجلس الأوروبي على أعضائه أربعة جرائم تتضمنها القائمة الاختيارية، وترك للدول الأعضاء حرية التصرف في أسلوب التجريم والعقوبة بالنسبة لجرائم هذه القائمة الاختيارية وهي تتضمن :

- تعديل برامج الحاسب الآلي أو بياناته .
- التجسس على أنشطة الحاسب .
- استخدام الحاسب بدون تصريح .
- استخدام برامج الحاسب المحمية بدون تصريح .

وقد استجابت معظم الدول الأعضاء لهذه التوصيات (Carr,1994) .

ويتضح من الحصر السابق أن جريمة مثل حذف بيانات الحاسب لم يتم تجريمها من قبل الاتحاد الأوروبي سواء في القائمة الإجبارية أو الاختيارية ، حيث الحذف لا يعتبر تدميرًا أو تزويرًا أو تخريبًا وفقًا لتعريف القانون البريطاني والاسكتلندي . كما يلاحظ أن نشر الفيروسات لم يعدها المشرع الأوروبي جريمة ، وربما كان ذلك لصعوبة ضبط مرتكبيها وإقامة الدليل عليهم . ونقترح هنا أن تضاف هاتان الجريمتان بوضوح إلى القائمة .

١٤ . ٣ . ٢ محاولات توحيد التشريعات

احتاج الاتحاد الأوروبي خمسة عشر عامًا من المناقشات والمداولات حتى انتهى إلى وضع مسودة إعلان النوايا التي مهدت الطريق لإصدار تشريع لتداول المعلومات ، وقد تم التوصل لهذه المسودة في عام ١٩٩٠ وتمت موافقة البرلمان الأوروبي على نسختها المعدلة في عام ١٩٩٢ (Official Journal,1992) في هذا الإعلان تم ولأول مرة حصر الحالات التي يكون فيها استخدام البيانات الشخصية قانونيًا ومباحًا وهي :

- أن يوافق على ذلك صاحب البيانات (المادة ٧ ـ أ) .
- أن يكون استخدام البيانات ضروريًا لإبرام تعاقد مع صاحب البيانات أو من أجل البت في طلب مقدم من صاحب البيانات قبل التعاقد معه (المادة ٧ـ ب) .

- أن يكون استخدام البيانات ضروريًا من أجل تنفيذ التزام يفرضه قانون الدولي أو قانون الاتحاد الأوروبي (المادة ٧ ـ ج).
- أن يكون استخدام البيانات ضروريًا لحماية المصالح الحيوية لصاحب البيانات (المادة ٧ ـ د).
- أن يكون استخدام البيانات ضروريًا لأداء مهمة تخدم الصالح العام، أو مهمة تقوم بها سلطة عامة تكون مكلفة بذلك أو تكون ضرورية لطرف ثالث يلزم أن تُكشف له هذه البيانات (المادة ٧ ـ هـ).
- أن يكون استخدام البيانات ضروريًا للمحافظة على الصالح العام أو للحفاظ على المصالح المشروعة لطرف ثالث يلزم أن تُكشف له هذه البيانات، ما لم تتعارض هذه المصالح مع مصالح صاحب البيانات نفسه (المادة ٧ ـ و).

١٤ . ٤ التشريع في الدول العربية

١٤ . ٤ . ١ ضرورة تجريم جريمة العصر

نقترح أن يأخذ موضوع تجريم جرائم نظم المعلومات وإصدار التشريعات والقوانين اللازمة لمكافحتها حقها من الدراسة في مؤسساتنا التشريعية العربية، حتى نستطيع التصدي لنوع جديد من الجرائم يُطلق عليه اسم «جريمة العصر» حيث لا توجد فيها آثار أقدام أو أقفال مكسورة أو بصمات أصابع، بل إن الضحية ربما قد لا يعرف بوقوع الجريمة وهذا أخطر ما في الأمر.

ونأمل أن تتبنى الدول العربية في تشريعاتها النص علي تجريم الاعتداء علي المال المعلوماتي المعنوي وذلك بإحدى وسيلتين: إما أن يقرر في نفس النص الذي يجرم الاعتداء على الأموال أن يعتبر المال المعلوماتي مالاً بالمعني التقليدي ويشمله بالحماية الجنائية في كل صور الاعتداء سواء بالسرقة أو

الإتلاف أو غيرهما، أو أن ينص علي كل جريمة علي حدة بالتجريم كما نص المشرع الفرنسي في القانون الجديد.

ونرى أنه لابد وأن يسرع المشرع في الدول العربية بالتدخل لسد الفراغ التشريعي الذي يعانيه هذا الموضوع وذلك بالنص علي تجريم بعض أنماط السلوك المخالف وذلك بإصدار قانون خاص يلحق بقانون العقوبات ليعالج هذه الظواهر المستحدثة.

كذلك يجب أن يراعي في صياغة القانون التقنيات الحديثة والاصطلاحات العلمية وقابلية ذلك للتغيير المستمر نتيجة للتطور المتلاحق والسريع في هذا الموضوع~، ولذا يجب الاستعانة بخبراء أمن الحاسب مع الخبراء القانونيين عند صياغة القانون.

كذلك فالمجرم المعلوماتي هو مجرم ذكي ذو مهارات تقنية عالية، لذا يجب التعامل معه بما لا يدع له مجالاً للإفلات من العقاب نتيجة صعوبة إثبات الواقعة.

١٤ . ٤ . ٢ هل تبدأ الدول العربية في التطبيق الفعلي والحازم لقوانين حماية الملكية الفكرية؟

يجري في معظم العواصم العربية في الوقت الحالي الكثير من المناقشات حول إقرار وتنفيذ قوانين حماية الملكية الفكرية أو حق المؤلف في مجال الحاسب الآلي ونعني بذلك في المقام الأول كتابة البرمجيات، وهذا الإقرار هو شرط من الشروط الهامة التي يجب أن تتوفر في أي دولة تسعى إلى الانضمام لمنظمة التجارة العالمية (وملحقاتها الهامة كاتفاقيات بيرن وتريبس) ونحن ندعو الدول العربية لى وضع وتفعيل قوانين تهدف إلى حماية الإنتاج والإبداع الفكري والإنساني من السرقة أو القرصنة.

١٤ . ٤ . ٣ مستقبل جرائم المعلوماتية والتشريع

من المؤكد أن مستقبل جرائم المعلوماتية مازال ممتدًا ومزدهرًا للأسف الشديد، وذلك نظرًا للتوسع في استخدامات الحاسب والإنترنت ودخول عالم التجارة الإلكترونية والاتصال عن بعد واحتمال ظهور أنماط جديدة للإجرام فيما بعد لذا يجب أن يتسم المشرع ببعد النظر وأن يستشرف التشريع الجديد آفاق المستقبل لكي يسمح بانطباق النص علي الصور المستحدثة~ التي قد تظهر في السنوات القادمة.

١٤ . ٥ الضوابط الدينية

من المهم أن يؤخذ الجانب الديني في الاعتبار عند مناقشة أخلاقيات تداول المعلومات كنوع من الضوابط الدينية التي تحكم أخلاقيات استخدام وتداول المعلومات، والتي تردع أي اتجاه لدى الأفراد نحو ارتكاب جرائم نظم المعلومات، فالملاحظ أنه توجد معلومات تقدمها جهات كثيرة بالمجان وشبكة الإنترنت متخمة بكميات هائلة من هذه المعلومات الصالح منها والمفسد. وينطبق هذا علي جميع أنواع العلوم والفنون من خلال ملايين المواقع التي يطلع علي محتواها أكثر من ستين إلي مائة مليون متصل بالشبكة يوميًا ويتضاعف عددهم بسرعة مخيفة. ومن ثم يجب أن نركز علي ضرورة وجود الضوابط الدينية والأخلاقية، فالذي لا وازع ولا ضمير له قد أتيحت له وسيلة سهلة للغاية في توصيل أفكاره ونشر مفاسده بالدرجة نفسها المتاحة أمام النافعين للناس، وقوانين الدول تختلف في ما تتبناه من أساليب للتحكم فيما ينشر عبر شبكة الإنترنت، والمحرمات تختلف من مكان لآخر. ويكتسب موضوع أمن المعلومات من الوجهة الدينية صبغة مختلفة فالمفهوم الديني لأمن المعلومات هو أمان المضمون بمعني أن يكون المحتوي من المعلومات لا شبهة عليه وأن يكون نافعًا للبشر أجمعين.

ونقل المعلومة بين طرف وآخر فإنه لا يصح شرعًا أو قانونًا أن يكون عليها متلصص أو أن يسرقها طرف ثالث لا حق له فيها، خاصة إذا أخذنا في الاعتبار ما ستحدثه الإنترنت في أعمال التجارة ونقل الأموال بين الناس . ومن الوجهة الدينية يجب حفظ حق صاحب المعلومة من ضرورة ذكر المرجعية والملكية له وإن تم اقتباس جزء أو كل المعلومات أو الترجمة عنها بلغة غير لغتها فضلا عن ضرورة التفاهم بين الطرفين في حال وجود تكلفة يطلبها الطرف المؤلف من الطرف المستفيد (Shihata,1999) .

والقيم الدينية التي يجب أن تحكم أخلاقيات استخدام وتداول المعلومات منها الدعوة إلي إصلاح النفس وإعلاء القيم وقهر نوازع الشهوات والفجور ـ الأمانة والصدق ـ آداب التربية الإسلامية وذلك لأن الدين يمثل مجموع القيم الأخلاقية الهادفة التي تأخذ بيد الإنسان إلي التقدم والتطور والتسامي وعمل الخير ونبذ الشر . ومنها أيضا تعويد الطفل علي الجد والاجتهاد والتفوق العلمي رغبة في خدمة دينه ووطنه وأمته الإنسانية والاهتمام بالجانب الخلقي والاعتماد علي النفس, بالإضافة إلي غض البصر لأن البعد نعمة كبري امتن الله بها عباده .

ومن شكر النعمة استخدامها فيما خلقت له فالعين للنظر إلي الكون والتأمل في مخلوقات الله وأنعمه والقراءة والاطلاع والتسابق إلي الاختراع والابتكار وإثراء العلم . هذا فضلا عن الدعوة بالحكمة خاصة وشبكة الإنترنت يستخدمها فئات عديدة من الملل وتكتب عن الإسلام من منطلقات متعددة ومن الأفضل أن نبدأ بعرض الوجه الحقيقي للإسلام وبيان فضائله والتمسك بفضيلة الجدال بالتي هي أحسن (Shihata,1999) .

الفصل الخامس عشر

التحقيق في جرائم نظم المعلومات

١٥ . ١ اختيار محققي جرائم نظم المعلومات .

١٥ . ٢ الأدلة في جرائم الحاسب .

١٥ . ٣ أدوات التحقيق .

١٥ . ٤ فحص مسرح الجريمة .

١٥ . ٥ كسر كلمة المرور .

١٥ . ٦ كسر الشفرة .

التحقيق في جرائم نظم المعلومات

خصصنا هذا الفصل للحديث عن التحقيق في جرائم نظم المعلومات، فنبدأ الفصل بالحديث عن مواصفات من يتصدى لمهمة التحقيق في هذا النوع الخاص جدًا من الجرائم، والفرق الفرعية التي يتكون منها فريق التحقيق. ثم نناقش أنواع الأدلة التي يمكن جمعها والاستفادة منها في جرائم المعلوماتية، وأين يبحث عنها فريق التفتيش. ننتقل بعد ذلك إلى الحديث عن الأدوات التي ينبغي على محقق جرائم نظم المعلومات أن يتسلح بها، ثم نقدم بعض النصائح التي يجب الاهتمام بها عند فحص مسرح الجريمة. ننتقل بعد ذلك إلى موضوعين هامين هما: كيفية كسر كلمة المرور، ومحاولة كسر الشفرة. وقد ترددت كثيرًا قبل أن أقرر إضافة هذا الجزء (بالذات عن كسر كلمة المرور) خوفًا من أن يستفيد منه المجرمون إلا أنني وجدت أن هذه المعلومات ربما يستطيع المجرمون الحصول عليها بوسائلهم الخاصة فرأيت ألا أحرم رجل الأمن من هذه المعلومات.

١٥ . ١ اختيار محققي جرائم نظم المعلومات

١٥ . ١ . ١ خلفية المحقق

المشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه، فمتخصصو الحاسب قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم إلى المحاكمة. وفي كثير من الحوادث نجد أن متخصص الحاسب يظن أن لديه الدليل الحاسم، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى.

بينما المحققون ذوو الخلفية القانونية، كرجال الشرطة مثلاً، قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم، وقد رأينا كيف أن أحد المحققين قد استدعى المتهم وأمره بالجلوس أمام الحاسب الشخصي موضوع الجريمة وطلب منه أن يريه الملف الذي قام بتزوير بياناته. فما كان من المتهم إلا أن قام بحذف هذا الملف بأمر واحد أدخله من لوحة المفاتيح، وضاع الدليل الرئيسي في الجريمة!!.

وفي حادثة أخرى تم القبض على بعض المتهمين وضبط (حاسب مركزي)، وقامت سلطات التحقيق بتفكيك الحاسب المركزي باعتباره دليل الجريمة وقامت بنقله إلى مركز الشركة. وهناك تبين أن تشغيل هذا الجهاز لفحص مكوناته يحتاج إلى تكييف هواء، وإلى تبريد ماء، وإلى إعادة توصيل الكابلات التي تم تفكيكها دون أن يتم ترقيمها، أي أن العمل المطلوب شبه مستحيل، وضاعت القضية كذلك.

من ناحية أخرى كان المتهم في إحدى الحوادث يدير «لوحة إعلانات إلكترونية» (Bulletin Board)، وهذه اللوحات من أهدافها الأساسية الحصول على البرمجيات الجديدة (Grabosky,1998). وكانت التهمة الموجهة إلى المتهم هي التجارة في الصور الفاضحة. فقام محققو الشرطة باستدعاء خبراء الحاسب لمحاولة العثور على الأدلة وتقييمها. فقام هؤلاء الخبراء بفحص القرص الصلب في جهاز المتهم، وخلال عملية الفحص قاموا بتحميل هذا القرص من أشرطة النسخ الاحتياطي الخاصة بالمتهم، ولم ينتبهوا إلى ضرورة أن يسبق ذلك البحث عن الملفات المخفاة، أو الملفات التي سبق مسحها من القرص الصلب الخاص بجهازه، وهكذا تم تدمير الأدلة قبل اكتشافها.

هذه المشاكل جميعها كان من الممكن تلافيها إذا كان لدى المحققين التدريب الكافي على التعامل مع مثل هذا النوع من الجرائم. التدريب على تقنيات الحاسب، والتدريب على أساليب التحقيق ومواد القانون. والجمع بين خلفية المحقق وخلفية متخصص الحاسب مهم جدًا لمن يريد التصدي للتحقيق في جرائم نظم المعلومات.

من الأمثلة السابقة يمكن أن نستخلص قاعدتين ذهبيتين: القاعدة الأولى هي ضرورة عدم إدخال أي تعديل على الوضع الذي تجد عليه الحاسب، والقاعدة الثانية هي ألا تسمح للمتهم باستخدام الحاسب موضوع الجريمة أو أي حاسب آخر متصل بالشبكة (Clark,1996).

١٥ . ١ . ٢ تكوين فرق العمل

العمل في التحقيق في قضايا نظم المعلومات يكون عادة أكبر من أن يتولاه شخص واحد بمفرده، حتى لو كانت المضبوطات هي مجرد حاسب شخصي واحد. ولذلك يفضل أن يتعاون عدة أشخاص في إنجاز مهمة التحقيق والعثور على الأدلة. ومن الضروري أن يكون لدى فريق التحقيق حاسب محمول ومثبت به بطاقة شبكة ليتمكنوا من أخذ نسخة احتياطية من محتويات الأجهزة التي قد يجدونها في مسرح الجريمة. وفيما يلي تصور عن فرق العمل التي تشارك في معالجة قضايا نظم المعلومات:

١٥ . ١ . ٢ . ١ المحقق الرئيسي (ضابط القضية)

يجب أن تتوفر لدى المحقق الرئيسي خبرة واسعة في التحقيق في القضايا المعقدة، فهو يدير العمل ويوجه باقي المحققين ويتواجه مع وسائل الإعلام.

١٥ . ١ . ٢ . ٢ فريق الاستجواب

يتكون هذا الفريق من شخص أو أكثر، وتكون مهمتهم هي استجواب الشهود والمتهمين. ويجب أن تتوفر لديهم مهارات استجواب عالية.

١٥ . ١ . ٢ . ٣ فريق التصوير والرسم

يتكون هذا الفريق من أكثر من شخص، ويتولى مهمة تصوير كل المواقع داخل مسرح الجريمة وخارجه، وتصوير أدلة الجريمة، كما يقوم برسم «الاسكتشات» للموقع. وبالطبع يجب أن يكون هذا الفريق مزودًا بكاميرات «بولارويد» للتصوير الفوري وكاميرات (٣٥مم)، ويفضل وجود كاميرات «فيديو» كذلك لأنه قد يكون من المهم جدًا في القضية الرجوع إلى بعض التفاصيل مثل هل كان القفل مركبًا على الباب عند اكتشاف الجريمة أم لا، وهنا يكون لكاميرا «الفيديو» التي (تمسح) المكان فائدة كبرى.

ونؤكد هنا أنه يجب على المحققين الانتباه إلى ما يقولونه خلال تصوير المكان بكاميرا «الفيديو»، فإن كل ما يقولونه سوف يتم تسجيله مع الفيلم وسيتم عرضه في قاعة المحكمة، وربما سبب ذلك لهم الإحراج.

١٥ . ١ . ٢ . ٤ فرق التفتيش

تتولى هذه الفرق تفتيش كل غرفة ويقومون بالتقاط الأدلة وترقيمها وتمييزها بعلامات لاصقة ملونة لسهولة العودة إليها بعد ذلك بواسطة فريق جمع الأدلة. وليس من الضروري أن تكون لدى أفراد هذا الفريق خبرة بالحاسب، بل يكفي توجيههم إلى الأغراض المطلوب البحث عنها وضبطها.

١٥ . ١ . ٢ . ٥ فريق المداهمة

هذا الفريق مسئول عن مداهمة المكان المشتبه به، ثم يتولى مسئولية

تأمين الدخول إلى المبنى وتأمين الأفراد والأدلة، ويتولون مهمة القبض على المشتبه بهم ونقلهم، وهم يكونون عادة من رجال الشرطة المحترفين.

١٥ . ١ . ٢ . ٦ فريق جمع الأدلة

هذا الفريق يجب أن يتكون من شخصين أو ثلاثة (حسب مساحة وازدحام المكان)، ويكون أحدهم محقق حاسب، والآخر من متخصصي الحاسب. يتولى هذا الفريق جمع الأدلة الفنية، وإدخال بيانات عن هذه الأدلة في الحاسب، وترقيم كل دليل ووضعه في حقائب بلاستيكية أو صناديق (حسب طبيعة الدليل)، وترقيم هذه الصناديق بعد تصوير ما بها من أدلة.

وهذا الفريق مسئول كذلك عن تحليل الأدلة، واتخاذ الإجراء المناسب بشأنها بعد مناقشة الظروف الخاصة مع ضابط القضية، كما يقومون بنسخ بيانات الحاسب المضبوط إلى وسط محمول (كالأشرطة أو الأقراص الصلبة المحمولة).

١٥ . ٢ الأدلة في جرائم الحاسب

من المعروف أن الأدلة الفنية المضبوطة في جرائم نظم المعلومات لها أهمية كبرى، وقد يكون فيه الفصل بين الإدانة والبراءة للمتهم، ويجب أن يعتني فريق التفتيش وفريق جمع الأدلة بتخزين هذه الأدلة في بيئة مناسبة حتى لا تفسد. والقاعدة الذهبية هنا هي أن المكان المناسب لحفظ الأدلة هو المكان المناسب لك، فإذا كان المكان مريحًا لك فسيكون مناسبًا للأدلة (من ناحية التكييف والتهوية طبعًا).

وسنتحدث فيما يلي عن أنواع هذه الأدلة وأين يبحث عنها فريق التفتيش.

١٥ . ٢ . ١ أنواع الأدلة

١ ـ أدلة ورقية : مثل مخرجات الطباعة والتقارير والرسوم البيانية .

٢ ـ أجهزة الحاسبات : وتتضمن معها ملحقات الحاسب من شاشات وغير ذلك .

٣ ـ الأقراص المرنة والأقراص الصلبة : وهي من أهم الأدلة لأنها تحتوي على البيانات وعلى المعلومات وعلى كلمات المرور وعلى الصور وعلى التقارير، وعلى «خطط ارتكاب الجريمة» مثلاً وغير ذلك .

٤ ـ أشرطة تخزين المعلومات : وتستخدم عادة لحفظ النسخ الاحتياطية .

٥ ـ القطع الإلكترونية : ومن بين القطع الإلكترونية التي يمكن أن تكون أدلة مهمة أجهزة الإرسال التي تكون في صورة قطعة إلكترونية ، ولذلك يجب الاهتمام بفحصها للتأكد من طبيعتها ، خاصة في قضايا التجسس . وقد يكون الدليل الحاسم في قضية ما هو قطعة إلكترونية ملقاة في صندوق مهمل في أحد زوايا الغرفة ، فربما تكون هي جهاز الإرسال الذي يمكِّن المجرم من إرسال معلوماته إلى من قام بتجنيده .

٦ ـ أجهزة «المودم» : والتي تستخدم في نقل المعلومات ، ويمتاز بعضها بإمكانية أن يعمل كجهاز الرد على رسائل الهاتف (Answer machine) ، مما يجعله دليلاً محتملاً بالغ الأهمية . وعند العثور على «مودم» يجب الاهتمام بتسجيل الكابلات المتصلة به عند ضبطه ، وكيف كانت متصلة بالحاسب أو الهاتف (مع التقاط وتسجيل رقم الهاتف) .

٧ ـ البرامج : وهي تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات .

٨ ـ الطابعات وأجهزة تصوير المستندات : وما قد تحتويه من أوراق مطبوعة أو مصورة أو ما هو مختزن في ذاكرتها من معلومات .

١٥ . ٢ . ٢ أماكن وجود الأدلة

من المهم توجيه فريق التفتيش إلى الأماكن التي يبحثون فيها عن الأدلة المحتملة ومن هذه الأماكن:

١ ـ شاشة الحاسب: هي الموضع المفضل للصق بعض الأوراق اللاصقة الصفراء الصغيرة التي تحمل بعض المعلومات مثل أرقام الهاتف، أو اسم الفهرس الذي يحتوي على المعلومات داخل الحاسب، أو كلمات المرور. فكثير من مستخدمي الحاسب يستخدمون كلمات مرور متعددة ويقومون بتغييرها باستمرار، ولذلك فالكثير منهم يلصق ورقة صغيرة على شاشة الحاسب لتذكيره ببعض هذه الكلمات.

٢ ـ بجوار الهاتف: عادة توجد بجوار الهاتف بعض أرقام الهاتف أو الفاكس، أو بعض الرسائل المختصرة، أو ملخص لمحادثة مهمة، أو أسماء بعض الشركاء.

٣ ـ حافظة النقود: تحتوي حافظة النقود عادة على بطاقات الائتمان، وبطاقات الهاتف، ومذكرات صغيرة، وأسماء الشركاء وأرقام هواتفهم، وكلمات المرور، وجدول المهام المطلوب إتمامها، وربما يوجد قرص مرن في الحافظة.

٤ ـ المفكرة الإلكترونية: بعد انتشار هذا النوع من المفكرات الإلكترونية، فهي أصبحت من أهم الأدلة التي يجب التحفظ عليها، فهي تحتوي على أسماء وأرقام هواتف وعناوين بريد إلكتروني، وعلى مواعيد ومذكرات مختصرة، وعلى تواريخ هامة وعلى أرقام حجز للسفر بالطائرة، وغير ذلك من المعلومات الهامة التي قد تكون مفيدة جدًا للتحقيق.

٥ - جيوب المتهم : يحمل الكثير من مستخدمي الحاسب بعض الأقراص المرنة في جيب القميص ، ويكون بها عادة الكثير من المعلومات ، ومع تقدم العلم فهناك الآن أقراص مرنة رخيصة تتسع لأكثر من مائة ميجا بايت من المعلومات ، ويمكن أن توضع بسهولة في جيب القميص .

١٥ . ٣ أدوات التحقيق

١٥ . ٣ . ١ برنامج إذن التفتيش

برنامج إذن التفتيش(Computer Search Warrant Program) هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات عنها ، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة ، والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين ، أو ظروف ضبط هذا الدليل ، ويجب أن يكون هذا البرنامج مع المحقق على قرص مرن أو قرص صلب محمول .

١٥ . ٣ . ٢ قرص بدء تشغيل الحاسب

يجب وجود قرص بدء تشغيل الحاسب (Bootable diskette) مع المحقق لإمكان تشغيل الحاسبات إذا كان نظام التشغيل فيها محميًا بكلمة مرور ، ويجب أن يكون القرص مزودًا ببرنامج مضاعفة المساحة (Double Space) ، فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب .

١٥ . ٣ . ٣ برنامج :XtreePro Gold

وهو برنامج معالجة ملفات ممتاز يمكن من العثور على الملفات في أي مكان على الشبكة ، أو على القرص الصلب ، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة . ويستخدم

لقراءة البرامج في صورتها الأصلية، كما يمكن استخدامه للبحث عن كلمات معينة أو عن أسماء ملفات أو غير ذلك.

١٥ . ٣ . ٤ برنامج: LapLink

وهو برنامج يمكن تشغيله من قرص مرن، ويسمح بنسخ البيانات من الحاسب الخاص بالمتهم ونقلها إلى قرص آخر من خلال المنفذ المتتالي (Serial port)، أو المنفذ المتوازي (Parallel port). وهذا البرنامج مفيد جدًا للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

١٥ . ٣ . ٥ رنامج كشف الفيروسات وتدميرها

أي برنامج من برامج مكافحة الفيروسات يمكن أن يؤدي الغرض، وتكمن أهمية مثل هذا البرنامج في ضمان حماية جهاز الحاسب الخاص بالمحقق.

١٥ . ٣ . ٦ برنامج: AnaDisk / Viewdisk

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كان أسلوب تهيئته. وهذا البرنامج توجد منه نسخة عادية تصلح للأفراد العاديين ونسخة خاصة لرجال الشرطة أو محققي الحاسب الآلي، ويمكن الحصول عليه من شركة (Sydex Software) بالعنوان التالي:

Box 5700 Eugene, OR 97405 USA .O.P

أو بالاتصال برقم هاتف: ٣٣٠٦-٦٨٣(٥٠٣).

١٥ . ٣ . ٧ برامج الدمج وفك الدمج: Pkzip

وتستخدم لفك دمج البرامج، فربما كان المتهم قد قام بدمج برامجه، وفي هذه الحالة لا يمكن الاطلاع عليها إلا بعد فك الدمج.

١٥ . ٣ . ٨ برنامج اتصالات مثل :Lantastic

وهو يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات.

١٥ . ٣ . ٩ مجموعة كاملة من المفكات والمفاتيح.

١٥ . ٣ . ١٠ جهاز لنسخ المعلومات إلى قرص صلب.

١٥ . ٤ فحص مسرح الجريمة

نوجز هنا بعض الإجراءات الواجب اتخاذها قبل مداهمة مسرح الجريمة أو أثناءها أو بعد الانتهاء من المهمة:

١٥ . ٤ . ١ معاينة الموقع

قبل مداهمة المكان المشتبه فيه يجب معاينة الموقع لمعرفة المداخل والمخارج والعدد المتوقع للأفراد بالداخل، والعدد المتوقع للأجهزة الموجودة ونوعياتها، والبرامج والملفات الموجودة وهل هي مشفرة أم لا. هذه المعلومات إذا تم الحصول عليها مسبقًا فإنها قد توفر كثيرًا من الوقت. ويفضل إعداد خريطة «كروكية» للمنطقة وللدور الذي تقع فيه الشقة المطلوب مهاجمتها، ومعرفة مداخلها الأمامية والخلفية.

ويجب ألا ينسى المحقق أن يحمل معه الأجهزة والبرامج الضرورية، والأدوات اللازمة لنسخ المعلومات.

١٥ . ٤ . ٢ تكوين فريق المداهمة

في هذه المرحلة يتم تخصيص الأفراد المطلوبين لكل فريق من الفرق

الفرعية، وتحديد مهمة كل منهم وواجباته، وقد سبق تحديد مواصفات هذه الفرق وخلفيات أفرادها في القسم السابق من هذا الفصل.

١٥ . ٤ . ٣ وضع خطة المداهمة

من المهم أن تكون خطة المداهمة بسيطة وواضحة يفهمها جميع المشاركين، كما يجب أن تكون مكتوبة ومصحوبة بالرسوم التوضيحية التي تبين اتجاهات الهجوم. ويجب مراجعة الخطة مع الفرق المختصة قبل التوجه إلى الموقع. ويجب أن تتضمن هذه الخطة النقاط التالية:

١ ـ الموقف: ويجب أن يتضمن ما سوف تواجهه الفرق المقتحمة وما الذي تبحث عنه.

٢ ـ المهمة: يجب أن يكون هدف العملية واضحًا في الخطة، هل هو القبض على المتهم متلبسًا أمام الحاسب؟ أم المطلوب هو الوصول إلى الحاسب في غير وجود صاحبه مثلاً؟.

٣ ـ التنفيذ: ما هي خطوات إتمام المهمة؟ وما هو الوقت المناسب للتنفيذ؟ (ربما كان قبل بدء ساعات العمل إذا كان الهدف شركة)، ومتى يكون الوقت مناسبًا للقبض على المتهم متلبسًا؟.

٤ ـ منافذ الدخول والهرب: تحديد منافذ الدخول والهرب مهم جدًا سواء لاستخدام القوة المهاجمة أو للتحسب من استخدام المجرم لهذه المنافذ.

٥ ـ وسائل الاتصال بين أفراد القوة: يجب تأمين وسائل الاتصال (الراديو أو الهاتف الجوال أو راديو السيارة)، ويجب أن تكون الترددات متفق عليها، وأرقام الهواتف المحمولة مخزنة في هذه الهواتف لسهولة الاتصال. كما أنه في بعض العمليات الكبيرة قد يكون تشفير المكالمات لتأمينها مهمًا للغاية.

١٥ . ٤ . ٤ إذن التفتيش

في مثل هذا النوع من جرائم التقنية يحتاج طلب إذن التفتيش المزيد من العناية والاهتمام عند إعداده حتى يحظى بالموافقة من جانب سلطات النيابة المخولة بمنح الإذن، وحتى لا يشكك دفاع المتهم في سلامة الإجراءات. ويجب عند كتابة الإذن عدم استخدام عبارات أو مصطلحات غير واضحة. كما يجب مراجعة طلب الإذن من جانب واحد ممن لديهم خبرة أوسع في هذه الأمور.

١٥ . ٤ . ٥ تنفيذ المهمة

يجب عدم الكشف عن موعد المداهمة أو أية تفصيلات بشأنها قبل التنفيذ، ولا داعي لقطع الكهرباء عن المبنى حيث يمكن لأجهزة الحاسب أن تعمل على البطاريات الجافة. يفضل استخدام التسجيل بالفيديو لتسجيل عملية المداهمة وعملية التفتيش، لأنه سيكون فيه الرد الشافي على جميع محاولات المحامين اللاحقة.

١٥ . ٤ . ٦ تأمين الموقع

يجب سرعة تحديد مواقع أجهزة الحاسب في المبنى وتحديد ما إذا كانت هذه الأجهزة متصلة بشبكة داخلية أو متصلة بشبكة خارجية مثل الإنترنت.

يجب عند تفتيش شركة مثلاً عدم ترك أجهزة الحاسب دون حراسة أثناء عملية التفتيش، بل لابد أن يلازم أحد أفراد القوة كل جهاز لعدم مسح البيانات عليه أو استخدامه كوسيلة لإنذار الشركاء. كما يجب اختيار المكان الذي سيتم فيه استجواب العاملين بعيدًا عن أجهزة الحاسب.

١٥ . ٤ . ٧ متابعة أداء الفرق لعملها

من مهمة الضابط المسئول عن العملية الإشراف على أداء الفرق لمهامها، والتأكد من عدم مواجهتهم أي مشاكل، وحل المشاكل عند ظهورها.

١٥ . ٤ . ٨ بعد المداهمة

قبل مغادرة الموقع يجب الاهتمام بمراجعة أخيرة للفرق، وبعد المغادرة يجب توثيق العملية، وتسجيل الدروس المستفادة للاستفادة منها في العمليات التالية.

١٥ . ٥ كسر كلمة المرور

ترددت كثيرًا قبل كتابة هذا القسم خوفًا من أن أضع في يد المقتحمين و المتسللين، دون قصد، أداة تسهل مهامهم غير المشروعة. ولكن كيف نحرم محققي الحاسب الآلي ورجال الشرطة ورجال مكافحة التجسس ومكافحة الإرهاب من الاطلاع على بعض الوسائل التي تمكنهم من خدمة العدالة؟ وفي النهاية رجح لدي الرأي الثاني، فما به من فوائد ترجح ما به من مساوئ.

وقد فضلت أن أعرض هذه الوسائل في صورة وقائع حقيقية حدثت بالفعل، ووردت في بعض المجلات المتخصصة أو الكتب أو حتى الصحف، حتى تكون الفائدة أكبر. فأسلوب التفكير في الحل مهم، وأسلوب اختيار الوسيلة المناسبة للموقف هو أيضًا مهم.

١٥ . ٥ . ١ كسر كلمة مرور مشغل لوحة الإعلانات الإلكترونية

حدثت هذه التجربة في الولايات المتحدة (Clarck,1996)، إذ كان

المشتبه به يعمل مشغلاً «للوحة إعلانات إلكترونية» (BBS)، وبعد الوصول إلى جهاز الحاسب الشخصي الذي يستخدمه في إدارة اللوحة الإلكترونية حاول محققو الشرطة العثور على كلمة المرور الخاصة بالمشتبه به فقاموا بأخذ نسخة احتياطية من محتويات القرص الصلب، وقاموا بكتابة برنامج يحاول تشغيل انسخة الاحتياطية، وبعد فحص ملف المستفيدين استطاع المحققون الوصول بسهولة إلى أسماء المستفيدين وأرقامهم، ولكن لم يمكن العثور على كلمة المرور الخاصة بالمشتبه به، خاصة وأنها كانت مشفرة. ولولا تشفير كلمة المرور لأمكن إضافة مستفيد جديد بكلمة مرور جديدة ثم تتبع هذه الكلمة داخل قاعدة بيانات المستفيدين حتى يتم معرفة مكانها، ولكن التشفير حال دون ذلك.

للوصول إلى كلمة المرور قام المحققون بإنشاء رقمين جديدين من أرقام المستفيدين لهم أسماء مختلفة ولكن لهم نفس كلمة المرور، وبهذه الطريقة وبتتبع كلمتي المرور المتشابهتين أمكن العثور على مكان وجود كلمات المرور على القرص الصلب، ووضع المحققون يدهم على كلمة المرور الخاصة بالمتهم في ملف المستفيدين، ثم قاموا بإحلال كلمة المرور السابق استخدامها مع المستفيدين الوهميين مكان كلمة المرور الخاصة بالمشغل (وهي مشفرة كما هي). وبذلك أمكن الدخول إلى الحاسب باستخدام اسم المشغل مع كلمة المرور الخاصة بالمستفيد الوهمي.

١٥ . ٥ . ٢ الحاسب الدفتري المسروق

هذه قصة حاسب دفتري (Notebook) تمت سرقته، وبعد فترة أمكن استعادته، وكانت مهمة المحقق هي إثبات أن هذا الحاسب قد تم استخدامه لمدة طويلة، وأنه لم تكن لدى المتهم النية لإعادته إلى صاحبه.

تم استعادة البيانات من الحاسب المسروق لفحصها، وباستخدام برنامج «كويكن» (Quicken) تبين أنه قد استخدمت كلمة مرور لحماية البيانات المسجلة على الحاسب، ولم تفلح محاولات الوصول إلى موضع كلمة المرور في ملفات البيانات.

قام المحقق باستخدام برنامج الفحص (Debugger)، وقام بتتبع هذا البرنامج للتعرف على ذلك الموضع في الذاكرة الذي يتم فيه اختبار صحة كلمات المرور التي يدخلها المستفيدون، حتى توصل إليه.

ثم عاد لاستخدام برنامج «كويكن» وبعد بضع ساعات أمضاها في تشغيل هذا البرنامج استطاع العثور على البرنامج المستخدم في اختبار صحة كلمات المرور، وتم تعديل البرنامج الأخير لكي يقبل أي كلمة مرور وليست كلمة مرور المشغل، وبذلك انفتح باب مغارة «علي بابا».

١٥ . ٥ . ٣ كسر كلمة مرور مدير الشبكة المحلية

نظام التشغيل «نتوير» الخاص بشبكات «نوفيل» يستخدم أسلوب تشفير في اتجاه واحد، أي دون الحاجة إلى فك الشفرة. إذ يتم تخزين كلمة المرور، بعد تشفيرها، في قاعدة بيانات المستفيدين (Bindery) الموجودة في جهاز الخدمة (Server). وعند دخول المستفيد إلى الشبكة يتم تشفير كلمة المرور التي يدخلها من الطرفية التي يستخدمها. ثم ترسل كلمة المرور المشفرة إلى جهاز الخدمة حيث تتم مقارنتها بكلمة المرور المشفرة المخزنة من قبل. ولذلك فلا مجال هنا لاستخدام برنامج (HEX editor) أو استخدام برامج تحليل الشبكات (Network Analyzer) في محاولة معرفة كلمة المرور. هذا فضلاً عن أن الوصول إلى قاعدة بيانات المستفيدين (Bindery) حيث تخزن كلمات المرور في جهاز الخدمة هي من حق مدير الشبكة (Network supervisor) وحده.

وهناك طريقتان فقط تستطيع بهما الحصول على صلاحيات مدير الشبكة دون معرفة كلمة المرور الخاصة به: الأولى هي استخدام برنامج إدارة الشبكة (NLM) المحمل على جهاز الخدمة لتغيير كلمة المرور إلى كلمة معروفة. الطريقة الثانية هي تعديل برنامج (SETVER.EXE) لتغيير اسم قاعدة البيانات (Bindery) مما يرغم جهاز الخدمة على إنشاء قاعدة بيانات بديلة جديدة ليس بها من المستفيدين سوى «الضيف» (gest)، و«مدير الشبكة» (supervisor)، وليس بها كلمات مرور. أي في الوضع الذي كان فيه النظام عند تركيبه أول مرة. بعد ذلك تستطيع الدخول بصفة مدير الشبكة، ومن ثم تقوم بتشغيل برنامج مثل (BINDREST) لاستعادة ملفات قاعدة بيانات المستفيدين الأصلية. وباعتبارك، في هذه اللحظة، مسجلاً كمدير للشبكة فستظل لك الصلاحيات الكاملة على النظام برغم وجود قاعدة بيانات مستفيدين جديدة، وهنا يمكن إما تغيير كلمة مرور مدير الشبكة أو تعريف مستفيد جديد ذي صلاحيات مكافئة لمدير الشبكة لتتمكن من إجراء تحقيقاتك بسهولة. وننصح بأن يقوم بهذه العملية خبير لديه خبرة في نظام التشغيل «نتوير»، لأنه إذا لم يكن الشخص الجالس أمام لوحة المفاتيح يعرف جيدًا ما يفعل فإنه يمكن أن يتسبب في مسح محتويات القرص الصلب على جهاز الخدمة.

١٥ . ٥ . ٤ الموظف الحانق

في إحدى الدول الأوروبية قام أحد موظفي إدارة الإطفاء، قبيل تركه العمل، بحماية وثائق الاستجابة للطوارئ بكلمة مرور لا يعرفها سواه. كانت هذه الوثائق مكتوبة باستخدام معالج الكلمات (Wordperfect). وأمكن حل هذه المشكلة وكشف كلمة المرور السرية باستعادة برنامج (WPCRACK) من شبكة الإنترنت (وهو موجود بالعديد

من المواقع على الشبكة)، وهذا البرنامج يستغرق حوالي ثانية ونصف ليكشف كلمة المرور التي تحمي أي وثيقة مكتوبة بمعالج الكلمات هذا .

وهناك على شبكة الإنترنت وفي الأسواق كثير من البرامج المخصصة لكسر كلمات المرور منها شركة (Access Data) .

١٥ . ٥ . ٥ الهندسة الاجتماعية

اشتبهت الشرطة في أن مدير إحدى لوحات الإعلانات الإلكترونية يقوم بتوزيع صور جنسية فاضحة من خلال هذه اللوحة. قام المحققون بفحص الأقراص وباقي الأدلة دون العثور على أي ملفات مريبة. وكان آخر الأدلة هو شريط يحتوي على نسخة احتياطية لمحتويات القرص، وقد تم إعداده باستخدام برنامج (PC-Tools) ولكنه كان محميًا، ليس بكلمة مرور واحدة ولكن بعدة كلمات مرور سرية، تتجاوز عشر كلمات مرور متتالية يلزم معرفتها! .

قام محققو نظم المعلومات بالشرطة بما يُسمى «الهندسة الاجتماعية»، أي محاولة تخمين كلمة المرور عن طريق تجربة بعض الكلمات التي تتعلق بالجوانب الشخصية والاجتماعية للمشتبه به، مثل اسمه وأسماء أفراد أسرته واسم الكلب الذي يقتنيه، والأسماء والكلمات التي كان يستخدمها عند ممارسة بعض ألعاب الكمبيوتر. وفي النهاية أمكن التوصل إلى جميع كلمات المرور اللازمة واستعادة الصور الإباحية من الشريط الاحتياطي .

١٥ . ٥ . ٦ خطوات كسر كلمات المرور

تلخص الخطوات التالية ما يجب القيام به إذا أردت كسر إحدى كلمات المرور:

١ ـ حدد نوع البرنامج المحمي بكلمة المرور، وأسلوب التشفير المستخدم إذا كانت كلمة المرور مشفرة.

٢ ـ ابحث عن موضع تخزين كلمة المرور على الجهاز.

٣ ـ أدخل أكثر من كلمة مرور معروفة ثم قارن بين النسخ المشفرة منها.

٤ ـ إذا كنت تعلم قبل الحصول على إذن التفتيش أن المشتبه به يحمي بعض الملفات المطلوبة باستخدام كلمة مرور، فيفضل تضمين أمر التفتيش المستخرج من النيابة أمرًا للمشتبه به بتسليم كلمات المرور لقوة المداهمة.

١٥ . ٦ كسر الشفرة

أرجو ألا يتوقع القارئ أن يجد هنا وصفة سرية سهلة وسريعة لكسر الشفرة، كثير من أجهزة الاستخبارات في دول العالم تتمنى ذلك، وكثير من دوائر الشرطة ومكافحة الجريمة لا تكره شيئًا مثل الملفات المشفرة والرسائل المشفرة وكلمات المرور المشفرة. بل سنتحدث هنا عن صعوبة كسر الشفرة. وإذا أراد القارئ مزيدًا من المعلومات عن أساليب التشفير وكيفية كسر الشفرة فإنني أحيله لكتاب «الحاسب وأمن المعلومات» (داود، ٢٠٠٠).

في مقدور المتسلل الماهر أو متخصص الكمبيوتر أن يكسر بعض أساليب التشفير البسيطة، أما أساليب التشفير الأكثر صعوبة فهي قد تتطلب متخصصًا في كسر الشفرة ليحدد الأسلوب المستخدم في التشفير. وإذا لم تنجح الأساليب العلمية في كسر الشفرة، فليس أمامك إلا اللجوء إلى الأساليب التقليدية للشرطة (لإقناع) المشتبه به بالإفضاء بكل ما تريد معرفته لكشف البيانات (وهذه الأساليب تختلف من دولة إلى أخرى، ولكنها وصفة قلما تخيب!). وإذا فشلت هذه الوسيلة أيضًا فهناك دائمًا «الهندسة

الاجتماعية» التي تحدثنا عنها، ولكن هذه الوسيلة قد تستغرق أيامًا أو أسابيع وتحتاج إلى كم كبير من الصبر.

تستخدم بعض البرامج أساليب عشوائية لاستخراج كلمة المرور، ويتم ذلك بمحاولة توليد كلمات مرور متوالية أو كلمات مأخوذة من قاموس اللغة (وهو موجود على أقراص مضغوطة ويمكن البحث فيه بسهولة كبيرة) حتى يمكن الحصول على النتيجة المطلوبة. ولكن هذه البرامج تحتاج إلى حاسبات سريعة لأنها قد تجرب ملايين أو آلاف الملايين من كلمات المرور حتى تصل إلى الكلمة المنشودة. وبعض المجرمين يستخدمون كلمات مرور مكونة من مزيج من الحروف الكبيرة والحروف الصغيرة لجعل الأمر أكثر صعوبة أمام هذه البرامج العشوائية.

١٥ . ٦ . ١ برنامج «الخصوصية الفائقة»

عندما نتحدث عن التشفير فلا يمكن أن نغفل برنامجًا شهيرًا هو برنامج «الخصوصية الفائقة» (Pretty Good Privacy) أو (PGP) وهو برنامج تشفير يستخدم أسلوب المفتاح العلني، وهذا البرنامج يوزع مجانًا في الكثير من مواقع شبكة الإنترنت، ويمكن لأي شخص استخدامه، وهو منشور بلغة المصدر ومتاح لمن يريد معرفة آلية التشفير ولمن يريد محاولة كسره. وليس من الصعب الالتفاف حول السرية التي يوفرها هذا البرنامج، لذلك فهو جيد على المستوى الشخصي فقط، أي لاستخدام الأفراد عند التراسل فيما بينهم.

ويمكن استخدام هذا البرنامج لتنفيذ ما يلي:

١ ـ إضافة توقيع رقمي لرسائل البريد الإلكتروني لتأكيد شخصية المرسل.

٢ ـ تشفير نص الرسالة.

٣ ـ تشفير الملفات الثنائية مثل الملفات المضغوطة (Zip files).

المراجـــــع

داود، حسن طاهر (٢٠٠٠)، «الحاسب وأمن المعلومات»، الرياض : معهد الإدارة العامة.

Alqady, Hamed Roshdy(1999) Biological side effects of electromagnetic Radiation Symposium on Modern technology Crimes, Cairo - Egypt.

ASIS,(1998) www.asisonline.org accessed on 19 March.

Bernstein, Terry et al(1996) Internet Security for Business, New York :John Wiley..

Bidzos, D. James (1992) Public Key Cryptography" Book chapter (Ch. 13 in "Computer Security Reference Book edited by Jackson, K.M. & Hruska, J.) Butterworth - Heinemann.

Blackley, Bob (1997)The Emperor's Old Armor, ACM New Paradigm Workshop. Lake Arrowhead, C.A.

Cale, Douglas,(1999) Computer Assurance Services Practice at Deloitte & Touch (WWW.dttus.com), accessed on 24 June.

Campbell, Dennis & Susan Catter (ed) (1997) International Information Technology Law,England: John Wiley.

Carr, Indira Mahalingam & Williams, Katherine S.(1994) Bytes in Computer Law Book Chapter one in Computers and law Edited by Carr, Indira & Williams, Katherine. Intellect Oxford - London.

Cavis, Randall et al (1996) A new View of Intellectual Property and Software, The Communications of the ACM.

Clark, Franklin & Ken Diliberto(1996) Investigating Computer Crime, CRC press, Florida.

Cohen, Fred (1996)Internet Holes, Part 9 : IP Address Forgery and How to Eliminate it, Network Security Journal, Elsevier Publishing.

Cohen, Frederic (1992) Computer Viruses Book chapter (Ch. 44 in Computer Security Reference Book edited by Jackson, K.M. & Hruska, J.) Butterworth - Heinemann.

Collier, P. A. & Spaul B. J. (1994) A Forensic Methodology for countering Computer Crime Book Chapter in Computers and law" Edited by Carr, Indira & Williams, Katherine. Intellect Oxford - London.

Dunnigan, James F. & Albert A. Nofi (1995) Dirty Tricks at War, Morrow and Co..

Fay, Stephan (1992) The Collapse of Barings, w.w. Norton.

Ferbranche, D. (1992) Pathology of Computer Viruses, Springer-Verlag.

Grabosky, Peter Nils & Russell G. Smith (1998) Crime in the digital age: Controlling telecommunications and cyberspace illegalities, Australian Institute of Criminology, Australia..

Highland, Harold Joseph (1990) Computer Virus Handbook Elsevier Advanced Technology Oxford U.K.

Hoeren, Thomas (1994)Electronic Data Interchange: the Perspectives of Private International Law and Data Protection Book Chapter in Computers and law Edited by Carr, Indira & Williams, Katherine. Intellect Oxford - London.

HongKong Trader (1999) Bank launches Internet payment system, Hong Kong Trader.

Hutt, Arthur E. et al (1995) Computer Security Handbook 3rd edition, John Wiley & Sons.

Kantrow, Alan (1999) Knowledge Management definition of Monitor Company (WWW.monitor.com) accessed on 26 June.

Lejk, Mark and Deeks, David (1998) An introduction to Systems Analysis Techniques Prentice Hall.

Leveson, Nancy G. & Clark S. Turner (1993)An Investigation of the Therac-25 Accidents, IEEE Software.

Levy, Steven (1984) Hackers, Anchor / Doubleday.

Liu, Cricket et al (1994)Managing Internet Information Services OReilly & Associates.

Lutfy, Mohammed Hussam (1999)Information Awareness Symposium on Modern technology Crimes, Cairo - Egypt .

Masland, Molly (1999)The Dark Side of Online Shopping , http:\\www.msn.bc accessed on June,24.

Nachenberg, Carey(1997)Virus Protection techniques, ACM Communications Journal.

Official Journal (1992) Revised Draft Directive, No. L123, May, 8.

Parker, Donn B. (1976) Crime by Computer, Charles Scribner's Sons.

Parker, Donn B.(1998),Fighting Computer Crime'WILEY.

Pfleeger, Charles P. (1997) Security in Computers 2nd edition, Prentice Hall.

Rankin, Bob (1996) Dr. Bob's Painless guide to the INTERNET ,William Pollock Publisher.

Seidler, Lee et al (1977)The Equity Funding Papers, John Wiley & Sons, NewYork.

Shihata, Abdullah (1999) Religious Controls Symposium on Modern technology Crimes, Cairo - Egypt .

Shimmin, Bradley (1997)Effective E-Mail Academic Press Prfessional.

Sterling, Bruce (1996)The Hacker Crackdown, Bantam.

Stoll, Clifford, (1989)The Cuckoo's Egg , Bantam Doubleday Dell Publishing Group.

Weatherford, Jack (1997)The history of Money, Crown.

Wilding, Edward (1997) Computer Evidence: A Forensic Investigations Handbook, Sweet & Maxwell, London.

Xerox (1999) Report shown at (WWW.parc.xerox.com), 28 June.

الاخراج الفني والطباعة ـ مطابع أكاديمية نايف العربية للعلوم الأمنية ـ الرياض ـ هاتف: ٢٤٦٠٠٤٥

ردمك: ٩٩٦٠ ـ ٨٥٣ ـ ٠٦ ـ ٣